VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

BUDOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ NA FAKULTĚ PODNIKATELSKÉ

BUILDING SECURITY AWARENESS AT THE FACULTY OF BUSINESS AND MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jana Volfová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Jana Volfová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Budování bezpečnostního povědomí na fakultě podnikatelské

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vytvoření metodiky a pravidel pro soustavné budování bezpečnostního povědomí na fakultě podnikatelské.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky, Praha: Český normalizační institut, 2014.

NIST SP 800-50 Building an Information Technology Security Awareness and Training Program. Gaithersburg: National Institute of Standards and Technology, 2003.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Review of Cyber Hygiene practices. ENISA, 2016. ISBN 978-92-9204-219-6.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D.
ředitel

doc. Ing. Vojtěch Bartoš, Ph.D.
děkan

Abstrakt

Tato diplomová práce se zaměřuje na budování bezpečnostního povědomí na Fakultě podnikatelské. Skládá se ze tří základních částí, a to části teoretické, analytické a části s vlastními návrhy. Teoretická část obsahuje vysvětlení a objasnění některých základních pojmů, procesů a analýz, aby čtenář práci rozuměl. Část analytická obsahuje jak popis vybrané organizace, tak i konkrétní provedení analýz, které byly představeny v teoretické části. Poslední část, kterou je část praktická, obsahuje mimo jiné také vlastní návrhy průběhu zvyšování povědomí na fakultě a benefity tohoto procesu.

Klíčová slova

budování bezpečnostního povědomí, informační bezpečnost, kybernetická bezpečnost, systém řízení informační bezpečnosti, data, osobní údaje

Abstract

This diploma thesis is focused on Security Awareness Education at the Faculty of Business and Management. It consists of three main parts: theoretical, analytical and practical considerations. The theoretical part is the introduction to basic terms, processes and analysis to help understand the thesis. The analytical part includes an introduction to the chosen organization and the implementation of analysis, which were presented in the theoretical part. The practical part contains, among other things, the actual proposals for Security Awareness Education at the faculty and its benefits.

Key words

Security Awareness Education, information security, cyber security, Information Security Management System, data, personal data

Bibliografická citace

VOLFOVÁ, Jana. *Budování bezpečnostního povědomí na fakultě podnikatelské* [online]. Brno, 2021 [cit. 2021-05-13]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133635. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně

……...

Podpis studenta

Poděkování

Můj velký vděk patří panu Ing. Petrovi Sedlákovi za vedení mé diplomové práce, za jeho cenné a odborné rady, za jeho čas a pomoc při zpracování této práce. V neposlední řadě patří mé poděkování rodině, přátelům a známým, kteří mě při psaní této práce podporovali.

Obsah

Úvod

Cílem této práce je zvýšení povědomí o informační a kybernetické bezpečnosti na Fakultě podnikatelské. Výsledkem práce by mělo být jak vyšší povědomí, ale také proškolený personál a vybraní uživatelé. Všechny zainteresované strany by měly by být dostatečně informovány. Postup dosažení dostatečné informovanosti a vzdělávání zainteresovaných stran je obsahem této diplomové práce.

Prvním oddílem, který tvoří základ této práce, jsou teoretická východiska. Tato část obsahuje vysvětlení základních pojmů, které jsou v práci využity, představení systému řízení informační bezpečnosti, které je následované seznamem norem a standardů, které budou implementaci programu pro budování bezpečnostního povědomí ovlivňovat. Následuje kapitola o samotném programu, ve které jsou vymezeny modely, fáze programu, jeho životní cyklus a rozdělení klíčových rolí. Je zde zmínka o stanovení strategie programu a tvorbě a šíření vzdělávacích materiálů. Další kapitolou v pořadí je bezpečnostní politika. Následující kapitoly se věnují vysvětlení funkčnosti a přínosů Lewinova modelu, analýzy rizik, časové analýzy a analýz okolí organizace, kterými jsou analýzy SLEPTE, PORTER, 7S a SWOT.

Druhým oddílem je analýza problému a současné situace. V první řadě bude představena vybraná organizace, kterou je Fakulta podnikatelská, a její organizační struktura. Následuje provedení analýz, které byly představeny v teoretické části. Jako první je provedena analýza vnějšího okolí, po ní je provedena analýza oborového okolí, pak analýza interních faktorů. Analýza vnitřních a vnějších faktorů pak vychází z těchto tří analýz. Na závěr analytické části bude provedena analýza rizik. Její součástí je identifikace a ohodnocení hrozeb, které by mohly v průběhu realizace projektu nastat, jsou vytvořeny mapy rizik pro přehledné zobrazení jejich úrovně. Na konci analýzy rizik je podkapitola s protiopatřeními proti rizikům a jejich nová úroveň.

Posledním oddílem jsou vlastní návrhy řešení programu. Tato část začíná zpracováním Lewinova modelu, jehož součástí je analýza, zda vybranou změnu provádět, nebo ne, jsou zde zmíněny oblasti fungování fakulty, kterých se změna dotkne a bude zde poprvé zmíněn seznam činností, jež je potřeba vykonat, aby byl proces změny správně dokončen. Další kapitola se věnuje zpracování časové analýzy, kde je vytvořen síťový graf, ze

kterého je možné vyčíst předpokládanou délku trvání projektu včetně činností, které se nesmí opozdit, jinak by se délka trvání projektu prodloužila. Od třetí kapitoly v tomto oddílu se práce již věnuje budování bezpečnostního povědomí. Je zde zmíněn cíl, stanovena strategie, včetně určení rolí a jejích odpovědností a je stanovena frekvence opakování vzdělávání. Dále se zde nachází způsoby rozvoje podpůrných materiálů, včetně jejich témat, implementace. Důležitou kapitolou je finanční zhodnocení celého projektu. Poslední oddíl je zakončen kapitolou o post-implementační fázi, která se věnuje zpětné vazbě.

Práce je zakončena závěrem, ve kterém je shrnuta, jsou uvedeny její cíle a zda bylo těchto cílů dosaženo.

1 Teoretická východiska práce

Pro sjednocení výkladu nejčastěji používaných pojmů, které jsou v této práci používány, je potřeba hned na začátek stanovit jejich význam. První část tvoří teoretické základy práce, na kterých bude diplomová práce postavena.

1.1 Základní pojmy

Níže uvedené základní pojmy jsou vypsány spolu s anglickým ekvivalentem a vysvětlením jejich významu. Pro vysvětlení pojmů jsem vycházela z publikace Problematika ISMS v manažerské informatice a z normy ČSN ISO/IEC 27001:2014.

1.1.1 Pojmy

Aktivum (Asset) – veškerý hmotný a nehmotný majetek organizace (1, s. 15). Aktiva jsou tvořena HW, SW, službami a informacemi.

Analýza rizik (Risk Analysis) – systematické užívání informací, díky kterým lze odhadnout míru rizika a určit jeho zdroje (1, s. 16).

Audit (Audit) – nezávislý, dokumentovaný a systematický proces, který slouží k hodnocení dle stanovených kritérií (1, s. 16).

Autentizace – jde o poskytnutí záruky, že prohlašovaná charakteristika entity je správná (7).

Autorizace – znamená povolení k vykonání určitého výkonu či operace. Jde jak o samotné povolení, tak i o zjišťování, zda daný subjekt výkon či operaci může provést. V průběhu kontroly se obvykle navazuje na proces autentizace (8).

Bezpečnost informací (Information Security) – zachování integrity, důvěrnosti a dostupnosti informací (1, s. 13).

Bezpečnostní incident (Security Incident) – nežádoucí nebo neočekávaná událost nebo jejich série, které mohou s vysokou pravděpodobností způsobit poškození operací, které souvisí s činností organizace a ohrožení bezpečnosti informací (7)

Bezpečnostní politika (Security Policy) – pravidla, která určují postup, jak řídit, ochraňovat a distribuovat aktiva (1, s. 17).

Bezpečnostní událost (Security Event) – je už identifikovaný stav systému, služby nebo sítě, který poukazuje na možnost, že dojde k porušení bezpečnostní politiky nebo že dojde k selhání bezpečnostních opatření (1, s. 17).

CIO (Chief Information Officers) – lze přeložit jako vedoucí IT oddělení. Má odpovědnost za řízení, implementaci a využitelnost informačních technologií a počítačových systémů, které podporují cíle organizace (52).

CISO (Chief Information Security Officer) – jde v podstatě o manažera informační bezpečnosti. Ten odpovídá za informační bezpečnost v organizaci, má na starost na ni dohlížet, zlepšovat ji, plánuje rozvoj organizace, sleduje trendy, má za úkol sladit cíle organizace s cíli bezpečnosti (6).

Data (Data) – jsou „náplní" informace, kterou vytváří. Jde o opakovatelně interpretovatelnou podobu informace vhodnou pro komunikaci, vyhodnocení nebo zpracování (1, s. 12).

Dopad (Impact) – škoda, která vznikla v důsledku působení incidentu (1, s.16).

Dostupnost (Availability) – zajištění přístupu k informaci pro oprávněného uživatele (1, s.15).

Důvěrnost (Confidentiality) – data jsou dostupná pouze oprávněnému uživateli nebo procesu (1, s.15).

GDPR (General Data Protection Regulation) – je norma o ochraně osobních údajů. Představuje právní rámec, který má za úkol ochránit data před neoprávněným zacházením, což se týká i osobních údajů, a hájit tak co nejvíce práva občanů EU. GDPR zavedlo nejen vysoké pokuty za porušení nařízení, ale také některým správcům osobních dat nařídilo vytvořit nezávislou kontrolní funkci DPO, což je člověk, který kontroluje dodržování GDPR (9).

Hrozba (Threat) – možná příčina nechtěného incidentu. Výsledkem tohoto incidentu může být poškození organizace nebo systému (7).

Informace (Information) – širší pojem, který popisuje formou údajů reálné prostředí, jeho stav a procesy, které v něm probíhají. V informatice je informace tvořena kódovanými daty (kódování je způsob přepisu dat v zařízení nebo na přenosovém médiu) (1, s.12).

Informační bezpečnost (Information Security) – řeší ochranu a dostupnost informací, zahrnuje práci s daty v nedigitální formě (1, s. 13). Je řešená na úrovni organizace (jde o organizační, personální, komunikační a fyzickou ochranu). Informační bezpečnost je vlastně ochrana před poškozením, zničením či ztrátou dat, a to z hlediska dostupnosti, integrity a důvěrnosti (15).

Integrita – zajištění správnosti a úplnosti dat (1, s. 15).

Kybernetická bezpečnost (Cyber Security) – je typ informační bezpečnosti a týká se kybernetického prostoru. Jde o souhrn právní, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany kybernetického prostoru (15).

Kryptografie (Cryptography) – jedná se o vědní obor, který se zabývá způsoby utajení (šifrování) zpráv, a to převodem jejich obsahu do podoby, která je čitelná pouze se speciální znalostí (šifrovacím klíčem) (44).

Opatření (Countermeasure) – činnost, která umožňuje snížení dopadu rizika (1, s.16).

Osobní údaje (Personal Data) – osobní údaje představují jakékoliv údaje o fyzické nebo právnické osobě, kterou lze identifikovat podle určitého údaje. V rámci fyzické osoby se jedná především o jméno, věk, datum narození, ale též například fotografický záznam či IP adresu. Pro právnickou osobu jsou citlivými údaji například emailová adresa, telefonní číslo nebo identifikační údaje vydané státem (10).

Pravděpodobnost (Probability) – je možnost, že něco nastane (7).

Prohlášení o aplikovatelnosti (Statement of Applicability) – jde o dokument, který obsahuje prohlášení popisující bezpečnostní opatření a jejich cíle, která jsou aplikovatelná. Poskytuje popis, jakým způsobem se bude nakládat s identifikovanými riziky. Musí povinně obsahovat vybraná bezpečnostní opatření, důvod pro jejich výběr a cíle těchto opatření, bezpečnostní opatření, která v organizaci již fungují a jejich cíle a vyřazená bezpečnostní opatření včetně důvodu jejich vyřazení (1, s. 70).

Protiopatření (Countermeasures) – je postup, proces nebo cokoliv, co bylo speciálně navrženo, aby byla hrozba eliminována či snížena její působnost, aby se snížila zranitelnost nebo dopad této hrozby (31, s. 53).

Riziko (Risk) – jde o účinek nejistoty na dosažení cílů. Jedná se o odchylku od očekávání, která souvisí se znalostí události, jejího následku nebo pravděpodobnosti, že nastane (7).

Sociální inženýrství (Social Engineering) – je termín, který se užívá pro široký rozsah zlomyslných aktivit, které jsou prováděny skrze interakci s lidmi. Zneužívá psychologickou manipulaci, která vede k tomu, že cílová osoba či skupina udělá chybu a poskytne útočníkovi citlivé informace. (48)

Událost (Event) – výskyt nebo změna určité množiny okolností (7).

Zainteresovaná strana (Interested party) – tou může být osoba nebo organizace, kterou může rozhodnutí nebo činnost ovlivnit nebo na ni může mít vliv (7)

Zranitelnost (Vulnerability) – slabé místo aktiva (1, s.16).

1.2 Systém řízení informační bezpečnosti (ISMS)

ISMS je zkratkou pro anglický název Information Security Management System, což lze přeložit do češtiny jako Systém řízení informační bezpečnosti. Jedná se o řízení bezpečnosti informací včetně veškerých atributů, které to obnáší. ISMS je založeno na PDCA modelu a má 4 etapy (1, s. 14):

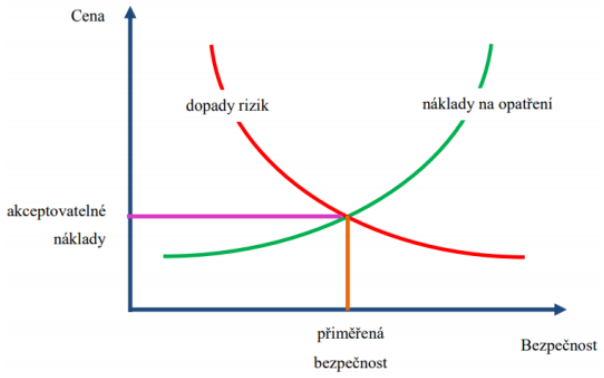
- Ustavení ISMS – v této části se určuje rozsah projektu a určují se odpovědnosti pro dílčí role, které se na ISMS budou podílet.
- Zavádění a provoz ISMS – zde se prosazují vybraná bezpečnostní opatření.
- Monitoring a přezkoumání ISMS – systém je již zaveden, je v plném provozu a je potřeba získat od uživatelů zpětnou vazbu včetně hodnocení, což má za úkol fáze číslo 3.
- Údržba a zlepšování – po zpětné vazbě se odstraňují nedostatky, slabiny a soustavně se systém zlepšuje. (1, s. 14).

1.2.1 Cíl ISMS

Cílem ISMS, jeho zavádění a převážně cílem provozu je efektivní a systematické prosazení vybraných bezpečnostních opatření.

Přiměřená bezpečnost

Přiměřená bezpečnost je přiměřená cena za zabezpečení. Je nezbytné chránit všechna data, nicméně taková ochrana stojí spoustu zdrojů, a to ať už jde o finanční, lidské nebo materiální zdroje. To, kolik se bude investovat zdrojů do bezpečnosti IS, musí odpovídat tomu, jak hodnotná aktiva organizace má a jaká rizika a v jaké míře mohou nastat.



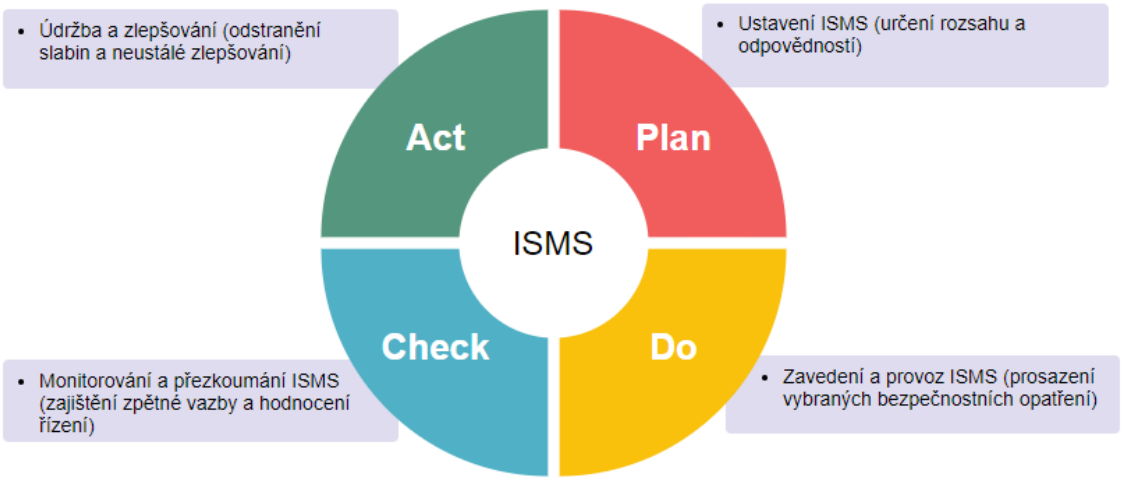
Obrázek 1: Graf přiměřené bezpečnosti
(Zdroj: 1, s. 36)

Jak lze z grafu vyčíst, tak náklady na opatření závisí na tom, jaké jsou dopady potenciálních rizik.

1.2.2 PDCA model

Jedná se o model, respektive metodu, která zajišťuje stálé zlepšování kvality výrobků, služeb, procesů apod. Smysl spočívá ve stálém opakování čtyř činností dokola.

- Plan (plánuj) – plánování záměru, proč PDCA model zavádět a proč jej využívat, v této části je potřeba procesy identifikovat.
- Do (dělej) – uvedení plánu do pohybu, jeho realizace, dochází k popsání a dokumentaci procesů.
- Check (kontroluj) – ověření, zda výsledek realizace odpovídá plánu. Je nutné řídit procesy na základě dokumentace z předchozího kroku.
- Act (jednej) – případná změna záměru a realizace plánu podle toho, zda výsledek v předchozím kroku odpovídal původnímu plánu. Plošná implementace zlepšení do praxe, dochází k optimalizaci průběhu činností (1, s. 24).



Obrázek 2: PDCA cyklus v ISMS
(Zdroj: Vlastní zpracování dle: 1, s.25)

1.3 Normy, zákony a standardy

1.3.1 Vysvětlení pojmů

Standard – zdokumentovaná domluva, která obsahuje technické specifikace, jež jsou důsledně používány jako pravidla, směrnice. Měly by zabezpečovat, že výrobky, služby,

procesy a materiály jsou takové, jak se zamýšlelo (např. formát kreditní karty, politika poskytování služeb apod.)

Norma – je doporučení pro daný standard. Konkrétně v ICT (Informační a komunikační technologie) se jedná o doporučení standardů, které jsou použitelné pro realizaci požadovaného řešení (1, s. 40).

1.3.2 Nadnárodní a celosvětové normalizační instituce

- ISO (International Organization for Standardization) – má na starosti podporu rozvoje standardizačních aktivit ve světě spolu s aktivitami souvisejícími. Organizace se zaměřuje na snazší mezinárodní směnu zboží a služeb a na spolupráci v rámci intelektuálních, vědeckých, technologických a ekonomických aktivit (1, s. 41).
- IEC (International Electrotechnical Comission) – připravuje a vydává mezinárodní normy, které spadají do oblasti elektrotechnických, elektronických a příbuzných oblastí, jako je například elektřina, magnetismus, multimédia, telekomunikace aj. (1, s. 41).
- ITU (International Telecommunications Union) – spadá pod OSN. Tato společnost se poslední dobou začíná soustředit na stavební prvky, které se objevují v globální informační infrastruktuře. Také se zajímá o tvorbu vyspělých multimediálních systémů, které umožňují sloučení hlasových, datových, zvukových a video signálů. (1, s. 41).

Tyto tři organizace, a to ISO, IEC a ITU, vydávají tzv. základní normy, které mají platnost na celém světě a při vypracovávání norem tyto organizace úzce spolupracují (1, s. 41).

1.3.3 Česká organizace

ČSNI (Český normalizační institut) – původně byl zřízen jako státní příspěvková organizace, nicméně dnes je již jednou z organizací, které jsou podřízeny Ministerstvu průmyslu a obchodu. Tato organizace má statut národní normalizační organizace, která zastupuje nadnárodní zájmy v mezinárodních a evropských normalizačních organizacích. Zaměřuje se především na tvorbu českých technických norem, jejich vydání a distribuci, poskytuje informace o těchto normách a v neposlední řadě spolupracuje s nevládními mezinárodními a evropskými normalizačními organizacemi (1, s. 44).

ČSN je česká technická norma, která může vzniknout dvěma způsoby:

- Přejímáním evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN IEC, ČSN ISO, ČSN ETS atd.).
- Tvorbou původních ČSN, které vyplývají z národních požadavků, potřeb a hledisek zachování funkčnosti fondu ČSN (1, s. 44).

1.3.4 Základní normy řady 27K

Normy ISO/IEC 27000 jsou rodina mezinárodních standardů, které se zaměřuje na informační bezpečnost a její řízení v organizacích. Tyto standardy jsou vydávány normalizační institucí ISO ve spolupráci s IEC.

ČSN ISO/IEC 27000:2010 – Přehled a slovník

Tato norma poskytuje přehled systémů řízení bezpečnosti informací a definuje související termíny. Obsahuje v podstatě přehled a slovník (1, s. 48).

ČSN ISO/IEC 27001:2006 - Požadavky

V současnosti existuje nejnovější vydání normy ICO/IEC 27001:2012. Tato norma specifikuje požadavky na ustavení, implementování, udržování a stálé zlepšování systému řízení bezpečnosti informací (1, s. 48).

ČSN ISO/IEC 27002:2006 – Soubor postupů

Tato norma obsahuje více jak 133 oblastí rozdělených do 11 kapitol, ve kterých lze nalézt více než 5000 přímých a odvozených bezpečnostních opatření, které pomohou dosáhnout podnikatelských cílů (1, s. 49).

ČSN ISO/IEC 27003:2012 – Směrnice pro implementaci systému řízení bezpečnosti informací

Norma poskytuje doporučení pro ustanovení a implementaci ISMS v souladu s požadavky normy ISO/IEC 27001. Výhodou je, že je norma použitelná pro všechny typy organizací. Vysvětluje proces návrhu a implementace ISMS, a to tak, že objasňuje průběh zahájení, definování a plánování projektu implementace ISMS. Výsledkem je finální plán (1, s. 50).

ČSN ISO/IEC 27004:2011 – Měření

Dává k dispozici doporučení pro vývoj a užívání metrik, pro měření, zda je zavedené ISMS účinné a jak moc a nabízí doporučení k měření účinnosti opatření, jak je uvedeno v ISO/IEC 27001 (1, s. 51).

ČSN ISO/IEC 27005:2009 – Řízení rizik bezpečnosti informací

Tato norma nabízí doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje koncept uvedený v ISO/IEC 27001 a je strukturována tak, aby dostatečně podporovala implementaci informační bezpečnosti (1, s. 51).

ČSN ISO/IEC 27006:2008 – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Norma specifikuje požadavky na orgány, které provádějí audit a certifikaci ISMS a nabízí doporučení pro tyto orgány (1, s. 51).

1.4 Budování bezpečnostního povědomí (SAE)

SAE (Security Awareness Education) je model pro budování bezpečnostního povědomí, který je založen na předpokladu, že učení se nikdy nekončící proces. V tomto případě začíná učení základní úrovní, povědomím, navazuje na něj trénink (školení) a rozvine se ve vzdělání, přičemž nejvyšší dosažitelnou úrovní je profesní rozvoj. V modelu jsou jasně určené role zainteresovaných stran a jejich odpovědnosti ve spojitosti s IT bezpečností. Náplní modelu je, mimo jiné, také stanovení úrovně, na které mají jednotlivé role dosáhnout. Úroveň povědomí o IT bezpečnosti vyžadují všechny role. Školení je doporučeno jednotlivcům, jejichž pozice v organizaci vyžaduje speciální znalosti hrozeb v oblasti v IT bezpečnosti, zranitelnosti a ochranných opatření vůči těmto zranitelnostem a hrozbám (45, s. 13-14).

1.4.1 Cíl SAE

Jedním z nejdůležitějších důvodů, proč informační bezpečnost v organizaci řešit, je ochrana aktiv organizace. Nejslabšími články v každém takovém řešení jsou vždy lidé, proto je nutné vytvořit metodiku, jak zainteresované strany vzdělávat a jak upevňovat jejich vědomosti v rámci informační bezpečnosti. Dalším z cílů SAE je zvýšení bezpečnostního povědomí. SAE je program, který má za úkol zvyšovat povědomí o informační a kybernetické bezpečnosti, zaměstnance a uživatele má za úkol školit a vzdělávat v této problematice. Nicméně primárním cílem tohoto programu je ochrana dat, informací a aktiv organizace s ohledem na důvěrnost, dostupnost a integritu. Primárního cíle bude dosaženo jedině tehdy, jestliže uživatelé a všichni lidé, kteří jsou do programu nějak zahrnuti budou:

- Rozumět svým rolím a odpovědnostem, které podporují cíl a misi organizace.

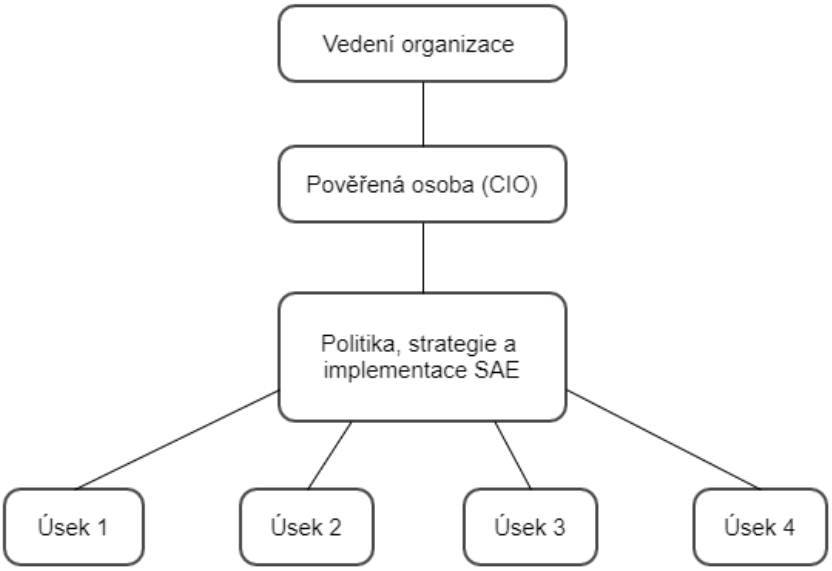
- Rozumět politice organizace, která se týká IT bezpečnosti, jejím činnostem a praktikám.
- Mít základní znalosti v rámci řídících, operačních a technických mechanismů, které jsou využívané pro ochranu informačních zdrojů, za které jsou zodpovědní (42, s. 1).

1.4.2 Modely SAE

Model SAE je možné navrhnout, rozvíjet a implementovat různými způsoby, ale existují tři nejčastější přístupy, kterých lze využít. Jsou jimi:

1) Centralizovaný model

Centralizovaná je jak politika, tak i strategie a implementace. V tomto případě má ústřední orgán zodpovědnost nejen za rozpočet, ale i za zpracování a návrh celého SAE. Veškeré plánování, řízení, strategie a zpracování dokumentace je na pověřené osobě. Tato osoba bude mít také za úkol vypracovat podpůrný materiál ke školení a vzdělávání. Komunikace je oboustranná, to znamená, že pověřená osoba komunikuje s organizačními jednotkami a naopak (viz obrázek). Centralizovaný přístup je většinou využíván malými společnostmi nebo takovými společnostmi, které mají vysoký stupeň struktury a ústředního managementu pro většinu funkcí IT nebo mají na úrovni vedení společnosti nezbytné zdroje, odbornost a znalost na potřebné úrovni (42, s. 12).



Obrázek 3: Centralizovaný přístup
(Zdroj: Vlastní zpracování dle 42)

2) Částečně decentralizovaný model

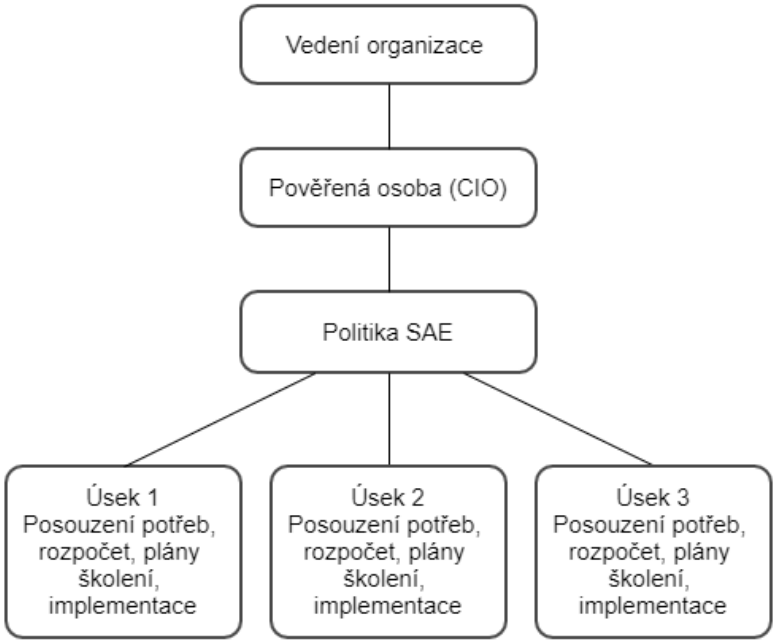
V modelu je centralizovaná politika a strategie, ale implementace je distribuovaná. To znamená, že bezpečnostní povědomí, školení, posouzení potřeb a strategie je definovaná pověřenou osobou, ale implementace je delegovaná na vedení jednotlivých úseků. Ti mají na starosti rozdělení rozpočtu na školení a produkty pro zvyšování bezpečnostního povědomí, zajištění materiálu a harmonogram. Komunikace mezi vedením organizace a jednotlivými úseky plyne oběma směry. Vedení může vyžadovat pravidelné hlášení od každého úseku ohledně rozpočtu, o plánech školení a o postupu implementace. Částečně decentralizovaný přístup je vhodný pro relativně velké organizace nebo pro ty, které mají spravedlivě decentralizovanou strukturu s jasnými odpovědnostmi, které jsou přiřazeny jak vedení, tak i jednotlivým úsekům. Je vhodný též pro takové organizace, které mají úseky s rozdílnými úlohami, což vede k potřebě značně rozlišit školení a vzdělávání podle toho, co jednotlivé úseky vyžadují (42, s. 13).

Obrázek 4: Částečně decentralizovaný přístup
(Zdroj: Vlastní zpracování dle 42)

3) Plně decentralizovaný model

V případě tohoto modelu pověřená osoba (CIO nebo manažer IT bezpečnosti) má na starosti vytvoření bezpečnostních politik, ale samotná implementace a tvorba strategie už je delegována na jiné uživatele. Tento model většinou vyžaduje rozdělení autorit do více

částí, kterým je nadřízená jedna centrální autorita. To znamená, že ve většině případů je potřeba vytvořit podsystém CIO a IT manažerů, kteří se zodpovídají nadřízenému CIO nebo vedoucímu IT oddělení. Jednotlivé úseky si také samy vytvářejí školící materiál. Plně decentralizovaný model se hodí pro takové organizace, které jsou relativně velké, mají silně decentralizovanou strukturu s rozdělenými odpovědnostmi jednotlivým členům vedení nebo jsou rozšířené po velké geografické oblasti (42, s. 15-16).



Obrázek 5: Plně decentralizovaný přístup
(Zdroj: Vlastní zpracování dle 42)

1.4.3 Fáze programu SAE

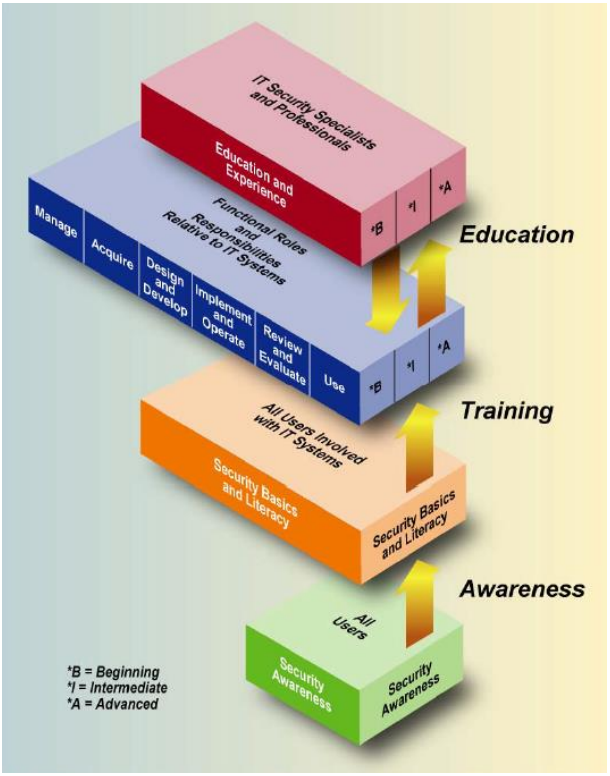
Program SAE je navržen tak, aby docházelo k neustálému učení uživatelů v oblasti bezpečnosti. Tito uživatelé během školení a vzdělávání získají nové zkušenosti a znalosti, které pak budou uplatňovat v praxi. Program je potřeba pravidelně aplikovat, přizpůsobovat ho novým trendům a aktualizovat. Existují čtyři úrovně vzdělávání v rámci SAE programu, přičemž každá se hodí pro jiný typ uživatele. Níže bude vysvětleno, v čem se liší a pro koho jsou vhodné.

Úrovně SAE programu:

- Povědomí
- Školení
- Vzdělávání

- Profesní rozvoj

Učení probíhá neustále, začíná povědomím o informační bezpečnosti, kde se uživatel dozví základy. Na to navazuje školení, které je následované vzděláváním (42, s. 8).



Obrázek 6: Fáze programu SAE
(Zdroj: Převzato z 42)

1) Povědomí

Podklady pro zvyšování povědomí by měly být vytvořeny tak, aby změnily chování uživatele, případně posílily jeho správné vědomosti a jeho chování v rámci bezpečnosti. Zvyšování povědomí není školení, ale jeho cílem je upozornit na to, že existují pojmy informační či kybernetická bezpečnost a co znamenají. Na této úrovni SAE programu je uživatel pouze příjemce informace a nemá prakticky žádnou aktivní roli. Zvyšování povědomí je cíleno na větší publikum, na větší počet lidí.

Vhodným příkladem pro přednášku nebo pro materiál ke zvyšování povědomí, který se bude šířit právě kvůli zvýšení povědomí, je například ochrana před viry. Lze v krátkosti vysvětlit, co to vir je, co se může stát, pokud virus napadne operační či informační systém, jaké kroky podstoupit pro to, aby takové nákaza nevznikla a co dělat v případě, je se systém virem nakažen (42, s. 9).

Příklady materiálů pro rozvor povědomí o IT bezpečnosti:

- Plakáty, letáky
- Video nahrávky týkající se bezpečnosti
- Reklamní/speciální předměty s motivačními slogany
- Spořiče obrazovky s tématikou IT bezpečnosti, které se ukážou, jakmile se uživatel z počítače odhlásí (45, s. 15).

2) Školení

Školení se od povědomí významně liší. Je více formální, má konkrétní cíl, a to úroveň vědomostí a znalostí potřebných pro výkon pracovní činnosti. Na úrovni školení se usiluje o to, aby si uživatelé vytvořili relevantní a potřebné vědomosti, znalosti a dovednosti v oblasti IT bezpečnosti. Největší rozdíl mezi povědomím a školením je v tom, že školení se snaží naučit uživatele určitým dovednostem, což mu pak umožňuje zastávat specifickou funkci. Kdežto povědomí cílí na pozornost jednotlivce v rámci konkrétního tématu či témat. Potřebné základy pro zúčastnění se školení jsou položeny již na první úrovni SAE programu, kterou je povědomí. Obsah školení musí být přizpůsoben oficiálním osnovám, které jsou vydávány pod taktovkou odborných institucí.

Příkladem školení může být kurz IT bezpečnosti pro systémové administrátory, který by se měl podrobně zabývat kontrolou řízení, kontrolou provozu a technickými kontrolami, které by v daném školení měly být zahrnuty. Kontrola řízení zahrnuje politiku organizace, program řízení IT bezpečnosti, řízení rizik a životní cyklus bezpečnosti. Kontrola provozu obsahuje personální a uživatelské potíže, pohotovostní plány, zvládání incidentů, povědomí a školení, počítačovou podporu a fyzické a enviromentální bezpečnostní problémy. Technická kontrola zahrnuje identifikaci a autentizaci, kontrolu přístupů a kryptografii (42, s. 9).

Školení lze rozdělit na tři části, přičemž každá část bude trochu jinak koncipovaná a bude se věnovat uživatelům ze tří různých kategorií:

A) Začátečníci
B) Středně pokročilí
C) Pokročilí

Uživatelé budou do jednotlivých kategorií rozřazeni na základě jejich vědomostí a znalostí.

3) Vzdělávání

Třetí úroveň SAE programu, a sice vzdělávání, slučuje všechny bezpečnostní vědomosti a znalosti z různých specializací do společného souboru znalostí. Usiluje tak o produkci specialistů a profesionálů na IT bezpečnost, kteří jsou prozíraví a proaktivní.

Jako příklad vzdělávání si lze uvést například studijní program na univerzitě či vysoké škole. Spousta takových škol a univerzit nabízí certifikované programy, které se skládají ze dvou, šesti nebo osmi kurzů a po složení tohoto programu získá student onen certifikát. Často tyto kurzy provádí škola ve spolupráci s prodejci hardwaru nebo softwaru (42, s. 10)

4) Profesní rozvoj

Tato úroveň by měla zajistit, aby uživatelé, měli požadovanou úroveň znalostí a dovedností, která je nezbytná pro jejich výkon. Tato úroveň je potvrzená certifikátem. Takový rozvoj a úspěšná certifikace mohou být nazvány jako „profesionalizace“. Přípravné práce pro testování takové certifikace většinou zahrnují studium předepsaného souboru znalostí nebo technických osnov. Tyto práce pak mohou být doplněny praxí na pracovišti. Kroky vstříc profesionalizaci v rámci IT bezpečnosti lze spatřit například mezi vedoucími pracovníky IT bezpečnosti, auditory IT bezpečnosti, systémovými nebo síťovými administrátory a oblasti se stále rozšiřují. Existují dva typy certifikací:

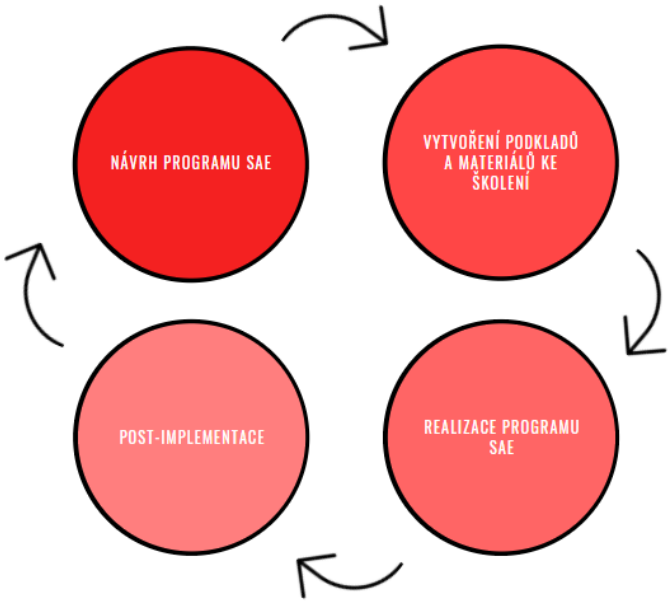
- Obecná – soustředí se na vytvoření základu znalostí týkajících se mnoha aspektů profese, která je prováděna v rámci IT bezpečnosti.
- Technická – primárně se soustředí na technické problémy bezpečnosti, které se týkají specifických platforem, operačních systémů apod. (42, s. 10).

1.4.4 Životní cyklus SAE

Hardware a software se vyvíjí neuvěřitelnou rychlostí, a to co platilo včera již dnes platit nemusí. Proto pro ochranu dat organizace, jejích aktiv a know-how, je nezbytné program SAE stále sledovat a aktualizovat. Bohužel nejde o jednorázovou akci, kdy se program zavede a od té chvíle již není potřeba se mu věnovat, kontrolovat jej či jej aktualizovat. Existují čtyři základní fáze životního cyklu programu SAE, kterými jsou:

- Návrh programu SAE – V tomto kroku se provádí posuzování potřeb organizace a dochází k návrhu a schválení školící strategie. Dokumenty ke školící strategii obsahují způsob implementace, který by měl být navržen tak, aby splňoval cíle školení.

- Vytvoření podkladů a materiálů ke školení – Jakmile je splněna první fáze cyklu, je možné přejít na další. Fáze se soustředí na dostupné zdroje školení, jejich obsah a rozsah, a rozvoj školících materiálů.
- Realizace programu SAE – Náplní této fáze je efektivní komunikace a zavedení SAE programu. Může navíc obsahovat způsoby použití materiálů pro školení a zvyšování povědomí (např. pomocí webu, video)
- Post-implementační fáze – Poslední část cyklu obsahuje návod, jak udržovat SAE program aktuální a jak sledovat jeho efektivitu. Jsou zde popsány efektivní metody zpětné vazby (např. průzkumy, dotazníky) (42, s. ES-1).



Obrázek 7: Životní cyklus SAE
(Zdroj: Vlastní zpracování dle 42)

1.4.5 Role a odpovědnosti v programu

Je nezbytné si pro potřeby diplomové práce stanovit role, které budou předem určeným osobám přiděleny, a jaké budou jejich odpovědnosti a povinnosti, co se SAE programu týče.

Vedení organizace

Vedení musí dohlédnout na to, že IT bezpečnosti bude přidělena vysoká priorita. To zahrnuje implementaci životaschopného bezpečnostního programu se silnými školícími a vzdělávacími komponenty.

Vedení organizace by mělo:

- Stanovit CIO.
- Přidělit odpovědnosti pro pracovníky IT bezpečnosti.
- Se ubezpečit, že implementovaný program pro IT bezpečnost zahrnuje všechny potřebné oblasti organizace, je vhodně podpořen zdroji (finančními, lidskými, materiálními) a je efektivní.
- Se ujistit, že má zaměstnance s potřebnými znalostmi a zkušenostmi pro ochranu IT zdrojů (42, s. 3).

Chief Information Officer (CIO)

CIO by měl spolupracovat s manažerem IT bezpečnosti:

- Na zřízení celkové strategie pro SAE program.
- Pro ujištění se, že vedení společnosti, vlastníci systému a dat a ostatní zúčastněné strany rozumí konceptu a strategii SAE programu a že jsou informováni o průběhu implementace tohoto programu.
- Pro ujištění se, že SAE program je financován.
- Pro zajištění školení a vzdělávání pro personál organizace, který má významnou zodpovědnost v rámci bezpečnosti.
- Pro ujištění se, že všichni uživatelé budou vhodně informováni a proškoleni.
- Pro ujištění se, že je implementován vhodný mechanismus pro sledování a reportování (42, s. 3-4).

Manažer IT bezpečnosti (CISO)

V rámci této role by se manažer měl:

- Ujistit, že školící materiály pro SAE program jsou vhodně a včas vytvořeny. s ohledem na publikum, kterému budou prezentovány.
- Ujistit, že uživatelé a manažeři mají k dispozici efektivní způsoby pro zpětnou vazbu vztahující se k SAE programu.
- Ujistit, že materiály jsou aktualizovány pravidelně, případně dle potřeby.
- Podílet na založení strategie pro sledování a reportování (42, s. 4).

Manažeři

Manažeři by měli:

- Spolupracovat s CIO a s manažerem IT bezpečnosti.
- Se ujistit, že všichni uživatelé jsou vhodně proškoleni a informováni, jak plně dostát své bezpečnostní odpovědnosti, a to před tím, než je jim umožněn přístup do systému.
- Pracovat na snížení chyb způsobených uživatelem z důvodu nedostatku znalostí, nebo z důvodu nedostatečného školení v rámci IT bezpečnosti.

Uživatelé

Tato skupina je skupinou největší a také nejdůležitější, co se snižování neúmyslných chyb a slabých míst bezpečnosti týče. Skupina uživatelů může zahrnovat zaměstnance, dodavatele, zahraniční či domácí hosty, zaměstnance jiných společností, návštěvníky, hosty, studenty a ostatní osoby vyžadující přístup do systému. Uživatelé musí:

- Pochopit a dodržovat bezpečnostní politiky a procedury.
- Být vhodně obeznámeni s pravidly chování v systému a aplikacích, ke kterým vyžadují přístup.
- Si být vědomi činností, které mohou lépe zabezpečit data organizace. Tyto činnosti zahrnují: vhodné heslo, zálohu dat, vhodný antivirový program, nahlášení podezřelých incidentů nebo narušení bezpečnostní politiky, dodržování pravidel, díky kterým se vyhnou útokům sociálního inženýrství a znemožní šíření se spamů či virů (42, s. 5).

1.4.6 Stanovení strategie a plánu SAE

Jakmile je dokončené posouzení potřeb, je možné se přesunout ke stanovení strategie pro rozvoj, implementaci a udržování programu SAE. Strategie je pracovní dokument obsahující prvky, které tvoří danou strategii. Těmito prvky jsou:

- Existující národní a místní politika (předpisy), která vyžaduje dokončení programu SAE.
- Rozsah SAE programu.
- Stanovení rolí a odpovědností osob, které se zabývají návrhem, zpracováním, implementací a udržováním školících materiálů.
- Stanovení cílů, kterých má být dosaženo pro každou úroveň programu (povědomí, školení, vzdělávání, profesionální rozvoj).

- Cílové skupiny pro každou úroveň programu.
- Povinné (a pokud bude možné, tak i doporučené) kurzy a materiály pro každou cílovou skupinu uživatelů.
- Témata pro každý kurz či školení.
- Metody implementace, které budou použity pro každou úroveň programu.
- Dokumentace, zpětná vazba a důkazy o školení – ty budou sloužit pro prověření, kdo už byl školen a komu školení ještě chybí.
- Hodnocení a update materiálů pro každou úroveň programu.
- Frekvence, s jakou by se měl výcvik v SAE programu opakovat (42, s. 19-20).

1.4.7 Metody šíření materiálů

Zvyšování povědomí

Existuje spousta způsobů, jak materiály šířit. Způsoby se většinou vybírají s ohledem na složitost informace, která se bude předávat, nebo s ohledem na zdroje, které jsou k dispozici (finanční, lidské, materiální). Příklady způsobů pro šíření materiálů:

- Poznámky na reklamních předmětech (jako například pera, klíčenky, deníčky, záložky, lékárničky, létající talíře apod.)
- Plakáty, checklisty, „to do“ listy
- Spořič obrazovky, vyskakující zprávy s upozorněními
- Noviny, video zprávy, videokonferenční schůzka
- Firemní emaily
- Odměnový program (plakety, hrnky, křížovky, děkovné dopisy)
- Kalendáře s informacemi a měsíčními bezpečnostními tipy
- Dny IT bezpečnosti či podobné události (42, s. 33)
- A další

Některé metody budou zahrnovat kratší zprávy, kratší úderná sdělení. Je tedy vhodné do nich zakomponovat hesla či text sepsat do pár odrážek. Jde převážně o spořiče obrazovky, vyskakující zprávy s upozorněními, odměnový program apod. Naopak v případě novin, „to do“ listů, video zpráv, checklistů aj. není potřeba se se zprávami držet tolik při zemi a lze se více rozepsat. Vzdělávací materiály je nutné udržovat aktuální a pro uživatele zajímavé. Je vhodné využívat více metod najednou, je pak větší pravděpodobnost, že si informace uživatelé zapamatují a vzdělávání pak pro ně bude i zajímavější (42, s. 33).

Školení

Před zpracováním materiálů pro školení je potřeba si položit otázku: „Jaké schopnosti chci, aby uživatelé získali a dokázali aplikovat?“. Školící plán by měl mimo jiné definovat typ uživatele, který školení potřebuje (42, s. 25). Rozdíl mezi materiály pro školení a pro zvyšování povědomí je takový, že materiály pro školení jdou do větší hloubky a následně je pak vyžadována a větší znalost. Metody pro efektivní šíření školících materiálů by měly využít výhody technologie, která podporuje následující funkce:

- Snadné užití (snadný přístup, jednoduchý update, snadná údržba)
- Škálovatelnost (lze použít pro různě velké školené skupiny na různých lokacích)
- Odpovědnost (užívání statistik k přehledu o stupni dokončení)
- Široká základna podpory (vhodné množství potenciálních prodejců, vyšší šance nálezu následné podpory) (42, s. 34)

Běžněji používanými metodami, které může organizace zahrnout, jsou:

- Interaktivní video trénink – jedna z mála technik, která využívá metodu distančního školení. Tato metoda podporuje obousměrnou komunikaci. Na obou stranách se využívá audio i video. Tato metoda je sice efektivnější než neinteraktivní metody, ale je podstatně dražší.
- Trénink ve webové aplikaci – poslední dobou jde o nejoblíbenější způsob školení, zvláště v rozdělených, různých prostředích. Uživatelé webové aplikace mohou studovat samostatně a svým tempem. Tréninkové modely, které zahrnují tuto metodu, začínají poskytovat navíc přidanou hodnotu, a to interakci mezi organizací a uživatelem, který je školen.
- Trénink založený na práci na počítači bez přístupu k internetu – stále populární metoda i přes to, že není možné využívat ke školení internet. Může jít o efektivní metodu pro distribuci školících materiálů, zvlášť, pokud přístup k materiálům, které jsou založeny na webové aplikaci, není proveditelný. Stejně jako v případě webových aplikací, tato metoda neumožňuje interakci mezi školitelem a uživatelem nebo mezi uživateli navzájem.
- Školení na místě s instruktorem – jedna z nejstarších, ale nejoblíbenějších metod pro šíření školících materiálů uživatelům. Největší výhodou této metody je přirozená interakce s instruktorem. Bohužel má tato metoda několik nevýhod.

> Ve velkých organizacích může být problém nalézt místnost dostatečně prostornou, aby pojala veškeré cílové skupiny školení. Pro organizace, které jsou geograficky více rozsáhlé, mohou být problémem značné cestovní náklady pro instruktory a uživatele (42, s. 34).

Pro udržení pozornosti uživatelů na školení lze zkombinovat různé metody dohromady, což může být zajímavý a efektivní způsob školení. Například je možné při školení na místě s instruktorem pustit výukové video, uživatelé tak budou mít k dispozici i jiný zdroj informací. Video může posílit informace, které už instruktor říkal, a zvýšit šanci jejich zapamatování (42, s. 34).

1.5 Post-implementační fáze SAE programu

Post-implementační fáze je poslední fází životního cyklu SAE programu, než začne celý cyklus od začátku. Program se může velice rychle stát zastaralým, pokud není věnována dostatečná pozornost technologickým pokrokům, IT infrastruktuře, organizačním změnám a změnám cílů organizace. Neustálé zlepšování v rámci IT bezpečnosti by pro organizaci mělo být vždycky aktuální téma, neboť se jedná o oblast, kde „nikdy nemůžete udělat dost“ (42, s. 35). Součástí této fáze je získání zpětné vazby od uživatelů a ostatních zúčastněných stran.

1.5.1 Hlídání dodržování programu

CIO a CISO by měli vytvořit hlídací program, který by měl zachytit klíčové informace co se aktivity týče (např. kurzy, data, ceny), a to prostřednictvím reportů. Tyto reporty mohou být využity pro identifikaci mezer a problémů v SAE programu, o které je možné se následně vhodně postarat například pomocí přidání vhodného školení či vzdělávání nebo založením vhodného plánu, jak tyto závady odstranit (42, s. 36).

1.5.2 Hodnocení a zpětná vazba

Jedná se o nejdůležitější část poslední fáze životního cyklu SAE programu a zahrnutí hodnocení a zpětné vazby do programu je přímo kritické. Bez zpětné vazby není možné, aby se program stále vyvíjel a zlepšoval. Způsob zpětné vazby musí být navržen tak, aby splňoval cíle, které byly původně stanovené pro program SAE. Existuje spousta různých způsobů, které je možné pro získání zpětné vazby využít.

Patří mezi ně například:

- Průzkumy, interview, nezávislá pozorování
- Benchmarking (nepřetržitý proces porovnávání a měření produktů, procesů a metod organizace zvoleným člověkem s cílem zlepšování aktivity organizace)
- Hodnotící formuláře a dotazníky
- Formální hlášení o stavu (42, s. 37-38)

1.5.3 Správa změn

Jedná se o součást programu, která by měla zajistit, aby obsah SAE programu nestagnoval, aby se stále vyvíjel a zlepšoval, aby byl stále relevantní a aktuální a odpovídal cílům organizace. Změny v cílech organizace mohou ovlivnit způsoby návrhu náplně školení a výběru míst pro školení. Je ale potřeba sledovat nejen průběh samotného programu, ale také okolí, které by tento program mohlo ovlivnit. Jde například o změnu v zákonech či vládní nařízení, která by program mohla ovlivnit a bylo by potřeba jej pak změnit a novým situacím přizpůsobit. To samozřejmě platí i o směrnicích, jejichž změna by se měla v návrhu SAE programu či jeho implementaci odrazit (42, s. 38).

1.5.4 Ukazatele úspěšnosti programu

Realizátoři programu, by měli být primárními osobami, které budou apelovat za to, aby se SAE program neustále zlepšoval. Důležité je si uvědomit, že ochrana dat a infrastruktury organizace je týmová práce a platí, že bezpečnost je tak silná, jak silný je její nejslabší článek. Existují klíčové ukazatele, které lze použít ke změření úspěšnosti programu. Jsou jimi:

- Dostatečné financování pro realizaci předem dohodnuté strategie.
- Vhodné organizační rozdělení tak, aby osoby s klíčovou odpovědností (CIO, CISO, osoby podílející se na řízení programu) mohly efektivně realizovat strategii.
- Podpora pro širokou distribuci (web, email, TV, rádio, studentský časopis apod.) materiálů pro zvyšování povědomí.
- Použití metrik (pro stanovení poklesu bezpečnostních incidentů a porušení, pro určení rozdílu mezi existujícím dosahem SAE programu a tím plánovaným dosahem, pro stanovení zvyšujícího se počtu uživatelů, kteří jsou v kontaktu se vzdělávacími materiály, vyjádřeného v procentech apod.)
- Výše návštěvnosti povinných školících kurzů.

- Motivace, kterou mají a prezentují osoby v pozici klíčových rolí (CIO, CISO, osoby podílející se na řízení programu).

1.6 Bezpečnostní politika

Bezpečnostní politika je právní dokument, který má na starosti popis, deklaraci a vysvětlení, jakým způsobem má organizace v plánu zajišťovat bezpečnost. Hlavním cílem této politiky je zachování nepřetržitě trvající provoz organizace tím, že napomáhá předcházet bezpečnostním incidentům nebo je pomáhá včas identifikovat, podchytit a řešit (49).

1.6.1 Cíle bezpečnosti informací

Fakulta podnikatelská musí určit cíle informační bezpečnosti, které jsou relevantní jednotlivým rolím a funkcím v organizaci. Cíle informační bezpečnosti musí:

- Být v souladu s politikou informační bezpečnosti.
- Být měřitelné, pokud je to možné.
- Brát v úvahu všechny požadavky na informační bezpečnost a výsledky z posuzování a ošetření rizik.
- Být komunikovány.
- Být aktualizovány podle potřeby (2, s. 10).

Při plánování, jakým způsobem budou cíle dosaženy, musí být jasně a srozumitelně zaznamenáno:

- Co se bude vykonávat.
- Jaké budou potřebné zdroje.
- Kdo bude za co zodpovědný.
- Kdy bude změna dokončena.
- Jakým způsobem budou vyhodnoceny výsledky (2, s. 10).

1.6.2 Politika

Vedení fakulty musí stanovit politiku informační bezpečnosti, která:

- Je přiměřená záměrům organizace.
- Zahrnuje buď cíle informační bezpečnosti, nebo poskytuje rámec, který bude využit k nastavení cílů informační bezpečnosti.

- Obsahuje závazek, který přislíbí splnění aplikovatelných požadavků, které se týkají informační bezpečnosti.
- Obsahuje závazek slibující neustále zlepšování systému řízení informační bezpečnosti (2, s. 8).

Politika informační bezpečnosti musí:

- Být dostupná jako dokumentovaná informace.
- Být komunikována v rámci organizace.
- Být přiměřeně dostupná zúčastněným stranám (2, s. 8).

1.7 Lewinův model

Lewinův model je jedním z nejznámějších modelů, které lze využít při řízení změn v organizaci. Má tři fáze, kterými jsou fáze rozmrazení, fáze přechodu a aplikace změny a fáze zmrazení. Jednotlivé fáze budou dále podrobněji vysvětleny a objasněny (50).

1.7.1 Fáze rozmrazení

Jedná se o rozmrazení stávajících pravidel a zvyklostí, následně dochází k určitým změnám (50). V této části je nutné připravit podmínky pro změnu či změny, provést nutné analýzy, komunikovat se zaměstnanci, připravit technologii firmy, zajisti zdroje. V první fázi je potřeba se materiálně, nehmotně, organizačně připravit na provedení změny (31, s. 34). Pro analýzu, zda změny provádět nebo ne, je možné využít metodu silového pole. Určit si toto pole, tedy síly, které působí pro a proti změně a ohodnotit je podle jejich důležitosti. Z této analýzy silového pole pak vyjde, zda je vhodné změnu realizovat či nikoliv. Následně budou popsány intervenční oblasti. Poslední částí v této fázi bude identifikace nositele změny. Dojde k určení agenta změny, sponzora změny a advokáta změny (31, s.32).

Intervenční oblasti

Intervenční oblasti jsou oblasti, ve kterých budou provedeny předem určené zásahy a dojde ke specifikaci těchto zásahů (intervencí). Intervence jsou směřovány do 4 oblastí:

- Lidské zdroje a jejich řízení
- Organizační struktura firmy
- Technologie firmy (z pohledu služby, produktu a doplňkových služeb)
- Komunikační a organizační toky a procesy firmy (31, s. 33)

Záleží pak na konkrétní změně, jak moc budou jednotlivé oblasti touto změnou ovlivněny.

Nositel změny

Ve skupině nositelů změny se nachází tři role, kterými jsou agent změny, sponzor změny a advokát změny. Každý z nich má svou funkci.

- Agent změny – Má na starosti danou změnu a odpovídá za její odborné provedení.
- Sponzor změny – Podporuje změnu svými finančními, materiálními a lidskými zdroji. Sponzor změny může být zároveň i agentem změny.
- Advokát změny – může být jednotlivec nebo skupina, které změna ovlivní, ale nijak do ní aktivně nezasahují (31, s.32).

1.7.2 Fáze přechodu a změny

Druhá fáze v pořadí, tedy fáze přechodu a změny, má na starosti vlastní provedení změny. Změna se bude zaměřovat na již zmíněné intervenční oblasti.

1.7.3 Fáze zmrazení

Po tom, co proběhne implementace změny, je potřeba danou změnu tzv. „zamrazit“, aby zůstala v takovém stavu, v jakém byla implementována. Pokud tato fáze nebude pořádně provedena, může dojít k nestabilitě prostředí a to se může vrátit do stavu, v jakém bylo před vykonáním změny. Dochází ke zpětné vazbě, hodnotí se dosažené výsledky, probíhá verifikace, zda byly zainteresované strany řádně proškoleny a jaký mělo školení přínos. (31, s. 35).

1.8 Analýza rizik

Analýzu rizik je potřeba provést pro započetí procesu snižování rizik. V rámci analýzy rizik probíhá definování hrozeb, stanovení hodnoty pravděpodobnosti, že tyto hrozby nastanou, a jaký by byl jejich dopad, kdyby nastaly.

Analýza většinou zahrnuje:

- Identifikace aktiv – identifikace organizace (nebo posuzovaného subjektu) a popis jejích aktiv.
- Stanovení hodnoty aktiv – určuje se, jakou hodnotu mají pro organizaci daná aktiva, hodnotí se možný dopad na organizaci, kdyby se aktiva ztratila, změnila nebo poškodila).

- Identifikace hrozeb a slabin – hledají se a určují slabá místa subjektu, která mohou zvýšit pravděpodobnost průběhu hrozby.
- Stanovení závažnosti hrozeb a míry zranitelnosti – stanoví se pravděpodobnost, že se daná hrozba vyskytne a určí se míra zranitelnosti subjektu vůči dané hrozbě (31, s. 50-51).

1.8.1 Metody analýzy rizik

Metody lze rozdělit například podle toho, jakým způsobem se vyjadřují veličiny, se kterými se v rámci analýzy pracuje. Z tohoto hlediska existují tři základní přístupy, kterými jsou:

- Kvantitativní – Tato metoda je nejpřesnější, protože je založena na matematických výpočtech a výsledky se obvykle vyjadřují ve finančních termínech (např. v tisících Kč). Jsou náročnější na provedení a zpracování výsledků
- Kvalitativní – Tento způsob je typický tím, že veličiny či hodnoty jsou vyjádřeny v určitém rozsahu (např. 1-10) nebo slovně (malý, střední, velký apod.). Úroveň je většinou stanovena odborným odhadem. Tato metoda je nejrychlejší, lehce pochopitelná, ale též dost subjektivní.
- Kombinované – Tato metoda kombinuje přesnější výpočty z kvantitativního způsobu, ale interpretace výsledků je vyjádřena kvalitativním způsobem, kvůli lepšímu pochopení (31, s. 67)

1.9 Časová analýza

Základem pro vytvoření časové analýzy projektu je stanovení si doby trvání jednotlivých činností, které jsou pro úspěšnost projektu potřebné. Jejich časovým ohodnocením se pak získá časově ohodnocený síťový graf.

1.9.1 Metody analýzy

Podle způsobu odhadu trvání činností se metody síťové analýzy dělí do dvou skupin:

1) Deterministické – stanovení doby trvání činností jako konstanty. Typickými představiteli tohoto způsobu jsou metody CPM a MPM
2) Stochastické – Doby trvání činností jsou stanoveny jako náhodné proměnné. Zástupcem tohoto způsobu je metody PERT (18, s. 106).

Podle způsobu interpretace činností (hran) dělíme grafy na:

1) Hranově definované síťové grafy
- Hrany – představují jednotlivé činnosti projektu
- Uzly – představují okamžiky zahájení nebo ukončení činnosti
2) Uzlově orientované síťové grafy
- Uzly – představují jednotlivé činnosti projektu
- Hrany – představují vazby mezi činnostmi

Cílem sestaveného grafu je nalézt a zobrazit nejkratší možný termín dokončení projektu, a to bez ohledu na typ grafu. Nejdelší cesta v grafu, což je cesta s nulovými časovými rezervami, která vede z počátečního do koncového uzlu, určuje nejkratší možný termín ukončení projektu (18, s. 107).

1.9.2 Metoda PERT

Pro potřeby této bakalářské práce byla pro zpracování časové analýzy, vybrána metoda PERT. Vybrána byla z toho důvodu, že není možné časově ohodnotit činnosti konstantami, vyskytovalo by se zde příliš vysoké riziko chybného odhadu. Doba trvání je v případě metody PERT brána jako náhodná veličina.

Odhad střední doby trvání činnosti

Počítá se pomocí vzorce: $t_{ij} = \frac{a_{ij}+4m_{ij}+b_{ij}}{6}$

a_{ij} = optimistický odhad trvání činnosti – nejkratší doba trvání, během které by za ideálních podmínek mohla být činnost dokončena.

m_{ij} = realistický odhad trvání činnosti – nejpravděpodobnější doba trvání činnosti (stanovena může být na základě zkušeností, statistiky apod.).

b_{ij} = pesimistický odhad trvání činnosti – nejdelší doba trvání činnosti, přičemž beze v úvahu veškeré překážky, které mohou činnosti zpozdit (18, s. 130).

1.9.3 Základní časové ukazatele

ZM = začátek možný – stanovuje, od jakého okamžiku zahájení realizace projektu je možné činnost nejdříve začít.

KM = konec možný – stanovuje nejdříve možný termín ukončení činnosti od zahájení projektu.

KP = konec přípustný – jde o nejpozdější termín, kdy je možné činnost ukončit, aby nebyl ohrožen časový plán projektu a nedošlo k jeho zpoždění.

ZP = začátek přípustný – nejpozdější termín, kdy lze zahájit činnost tak, aby nebyl ohrožen termín ukončení projektu a nedošlo k jeho zpoždění (18, s. 109).
RC = rezerva celková – vyjadřuje, o kolik lze odložit ZM činnosti nebo prodloužit její trvání, aniž by byl ohrožen celkový termín projektu (18, s. 113).

1.10 Analýza SLEPTE

Jde o analýzu vnějšího okolí podniku, která má na starosti analýzu okolí, které jej ovlivňuje. Díky tomu je organizace schopná lépe reagovat na změny, může cíleně provádět takové činnosti, které jsou smysluplné a naplňují její cíl, a může vytvářet harmonii mezi okolím a svou strategií. Analýza SLEPTE (občas lze narazit také na pojem PESTEL, ale jedná se o jednu a tutéž analýzu) se skládá z šesti faktorů, které ovlivňují vnější okolí organizace.

1.10.1 Sociální faktory

Ať už bereme v potaz jakoukoliv změnu v sociálním prostředí, téměř vždy tato změna může mít dopad na poptávku po produktech nebo službách organizace a je potřeba, aby organizace se o těchto změnách věděla a mohla se na ně nějakým způsobem připravit. Mezi sociální faktory patří například demografické změny (změna v populaci, posuny ve věku populace, rozložení příjmů populace), náboženské faktory, vzdělanost, rodinné hodnoty apod. (39).

1.10.2 Legislativní faktory

Do těchto faktorů spadají právní náležitosti prostředí, ve kterém se organizace vyskytuje. Jedná se o chystané a platné zákony a vyhlášky, které ovlivňují fungování zkoumané organizace, státní regulace a regulace importu a exportu (39).

1.10.3 Ekonomické faktory

Ekonomickými faktory jsou myšleny hlavně úrokové sazby, výše inflace a její dopad na ekonomiku, fáze hospodářského cyklu, směnné kurzy, nebo třeba regulace hospodářství (39).

1.10.4 Politický faktory

Politické faktory zahrnují vládní politiky, to, jak moc politika zasahuje do ekonomiky, jak hodlá podporovat podnikání. Mezi politické faktory lze zahrnout například aktuální politickou situaci, stabilitu státu a jeho pozici, podporu zahraničního obchodu apod. (39).

1.10.5 Technologické faktory

Technologické a technické faktory mají zásadní vliv na konkurenceschopnost organizace. Je nezbytné, zvlášť v dnešní době neustálého technologického pokroku, tyto faktory stále sledovat a přizpůsobovat se jim, jinak hrozí, že bude organizace zastaralá a nebude tolik atraktivní pro cílovou skupinu. Pod technologickými faktory si lze představit především postoj k vědě a výzkumu, jejich podporu a investice do tohoto odvětví (39).

1.10.6 Ekologické faktory

V posledních letech je na ekologii kladen čím dál větší důraz, tudíž je nutné se věnovat i těmto vnějším faktorům. Většina států jsou dokonce členy různých organizací, které slibují dodržování opatření, limitů a různých norem, co se ekologie a ochrany životního prostředí týče. Do ekologických faktorů lze zahrnout například odpadovou politiku (nakládání s odpady), přístup k ochraně životního prostředí, využívání obnovitelných zdrojů, ochranu ohrožených druhů aj. (39).

1.11 Analýza PORTER

Podstatou této analýzy je předvídání, jak bude vypadat budoucí vývoj konkurence a konkurenční situace daného odvětví. Analýza PORTER je analýzou oborového okolí a jejím úkolem je zjišťovat, jaký je stav v oboru, ve kterém se nachází zkoumaná organizace. Analýza zkoumá nejen úroveň konkurence a zda existující substituty výrobků či služeb, které organizace poskytuje a nabízí, ale také zda existují nějaké bariéry při vstupu nových konkurentů na oborový trh a jaká je vyjednávací síla dodavatelů a zákazníků (31, s. 36). Pomocí analýzy jsme schopní snížit vliv konkurence a v některých případech lze pro organizaci na trhu objevit nové příležitosti. PORTER analýza má pět faktorů, které ji tvoří. Jsou jimi:

1.11.1 Hrozba vstupu nových konkurentů

Vyjadřuje, jaká je možnost a jak vysoká, že na oborový trh, ve kterém se zkoumaná organizace vyskytuje, vstoupí nový konkurent a ovlivní tak cenu a nabízené množství výrobku nebo služby.

1.11.2 Hrozba stávajících konkurentů

Vyjadřuje, jaký vliv na oborový trh mají konkurenti, kteří se na něm již vyskytují, jak ovlivňují cenu a poptávané množství výrobku či služby.

1.11.3 Hrozba vzniku substitutů

Vyjadřuje, jak velká je pravděpodobnost, že se na daném oborovém trhu vyskytne výrobek či služba, která by mohla nahradit to, co poskytuje sledovaná organizace.

1.11.4 Vyjednávací síla zákazníků

Vyjadřuje pozici cílové skupiny, na kterou se sledovaná organizace orientuje na oborovém trhu, například zákazníků, a jejich schopnost ovlivnit cenu a poptávané množství po výrobku či službě.

1.11.5 Vyjednávací síla dodavatelů

Vyjadřuje, v jaké pozici jsou dodavatelé vůči sledované organizaci, zda dodavatelé mohou s organizací o ceně a množství komponentů vyjednávat či nikoliv.

1.12 Analýza 7S

Analýza 7S, nebo také McKinsey 7S, je analýzou interních faktorů. Analyzuje takové firemní oblasti, které jsou podstatné, důležité a nezbytné a které se přímo týkají organizace samotné (31, s. 39). Analýza byla navržena již v 70. letech 20. století a využívá se například při řízení změn, ve strategickém řízení či auditu (40).

1.12.1 Strategie

Má formu popisů aktivit a pokynů, aby bylo co nejlépe dosaženo předem určených cílů (například konkurenční výhody, uspokojení trhu apod.). Strategie primárně vychází z vize organizace a z jejího konkrétního poslání (31, s. 13).

1.12.2 Styl řízení

Existují tři styly řízení:

a) Autokratický – vylučuje podílení se ostatních pracovníků na řízení organizace. Zaměstnanci pouze mohou sdílet informace s vedoucím, nicméně rozhodování je pouze na něm (31, s. 20).
b) Demokratický – podřízení se mohou více začleňovat do řízení a chodu firmy a vedoucí delegují některé své pravomoci na zaměstnance. Komunikace je obousměrná, což znamená, že vedoucí informuje podřízené o svých záměrech a zároveň jim umožní vyjádřit svůj názor (31, s. 20).

c) Laissez-faire – zaměstnanci mají značnou volnost, komunikace probíhá primárně mezi členy skupiny (horizontální komunikace). Jedná se o nejliberálnější styl řízení organizace (31, s. 20).

1.12.3 Sdílené hodnoty

Jde o firemní kulturu čili seskupení nějaký představ, přístupů a hodnot v organizaci, které jsou všeobecně sdílené a dlouhodobě udržované (31, s. 23).

1.12.4 Spolupracovníci

Lidé, kteří jsou hlavním provozním rizikem, ale také hlavním zdrojem zvyšování výkonnosti. Je potřeba je správnými způsoby motivovat (31, s. 21).

1.12.5 Schopnosti

Jsou tím myšleny schopnosti pracovníků, které jsou tvořeny jejich znalostmi a dovednostmi (31, s. 24).

1.12.6 Systémy

Veškeré informační procedury, postupy a činnosti, které v organizaci probíhají (31, s. 20).

1.12.7 Struktura

Jde o správné a vhodné rozdělení kompetencí úkolů a pravomocí zaměstnancům organizace (31, s. 16). Existuje několik typů struktur organizace:

a) Liniová struktura – v organizaci se v rámci oddělení vyskytuje jeden útvar, který je nadřazen všem ostatním. Vyskytuje se zde přímá nadřízenost a podřízenost mezi útvary. Nevýhodou je potřeba vysoce znalých a zkušených vedoucích na jednotlivá oddělení (31, s. 16).
b) Funkcionální struktura – pokouší se o odstranění nedostatků, které má liniová struktura, což znamená, že jeden specializovaný nadřízený je nahrazen několika specializovaným vedoucími (31, s. 16).
c) Liniově štábní struktura – slučuje předchozí dva typy struktur do jedné. Vyskytuje se zde jak respekt potřeby jednotného vedení (liniová struktura), tak potřeba specializace a odbornosti (funkcionální struktura). Figurují zde samostatné útvary, štáby, které jsou podřízeny útvaru na vyšší úrovni. V ČR je tato struktura nejčastěji používaná (31, s. 16).

d) Divizionální struktura – organizace je rozdělena do divizí podle druhu výroby nebo služby, podle geografického umístění nebo třeba podle typu zákazníka (31, s. 16).
e) Maticové organizační struktury – slučuje prvky funkcionální a liniově štábní struktury. Můžeme zde narazit na možnost přímého kontaktu s vedoucím, tím je zvýšená motivace manažerů a je zde kladen důraz na skupinové práce. Nevýhodou mohou být konflikty mezi vedoucími, pokud se jejich názory neshodnou, nebo třeba nejasné zodpovědnosti za náklady a zisky (31, s. 16).
f) Hybridní struktury – většina organizací není schopná existovat pouze podle jedné struktury, existuje spousta modifikací, které se mohou měnit podle toho, jak se mění podmínky (31, s. 17).

1.13 Analýza SWOT

Tato analýza slouží ke zhodnocení vnějších a vnitřních faktorů, které ovlivňují působení organizace, její úspěšnost, případně úspěšnost konkrétní činnosti (41). SWOT analýzu tvoří čtyři faktory, kterými jsou:

Strengths – silné stránky organizace, v čem je dobrá, v čem vyniká

Weaknesses – slabé stránky, které organizaci nějakým způsobem škodí

Opportunities – příležitosti, které lze využít

Threats – hrozby, na které by si organizace měla dát pozor.

Tato analýza pokládá do protikladu faktory SW a OT, které mezi sebou můžeme vzájemně porovnávat a podle výsledků vyhodnotit. Faktory SW vychází z analýzy 7S, faktory OT vychází z analýz SLEPTE a Porter. Z výsledného hodnocení bychom se měli dozvědět, zda je vše v pořádku, nebo je potřeba nějaké opatření či změna. Analýza SWOT je relativně jednoduchý, ale mocný nástroj, který nám napomáhá upevnit silné stránky organizace, vylepšovat její slabé stránky, snižovat rizika, ideálně je minimalizovat a napomáhá nám také maximálně využít příležitosti organizace (41).

2 Analýza problému a současné situace

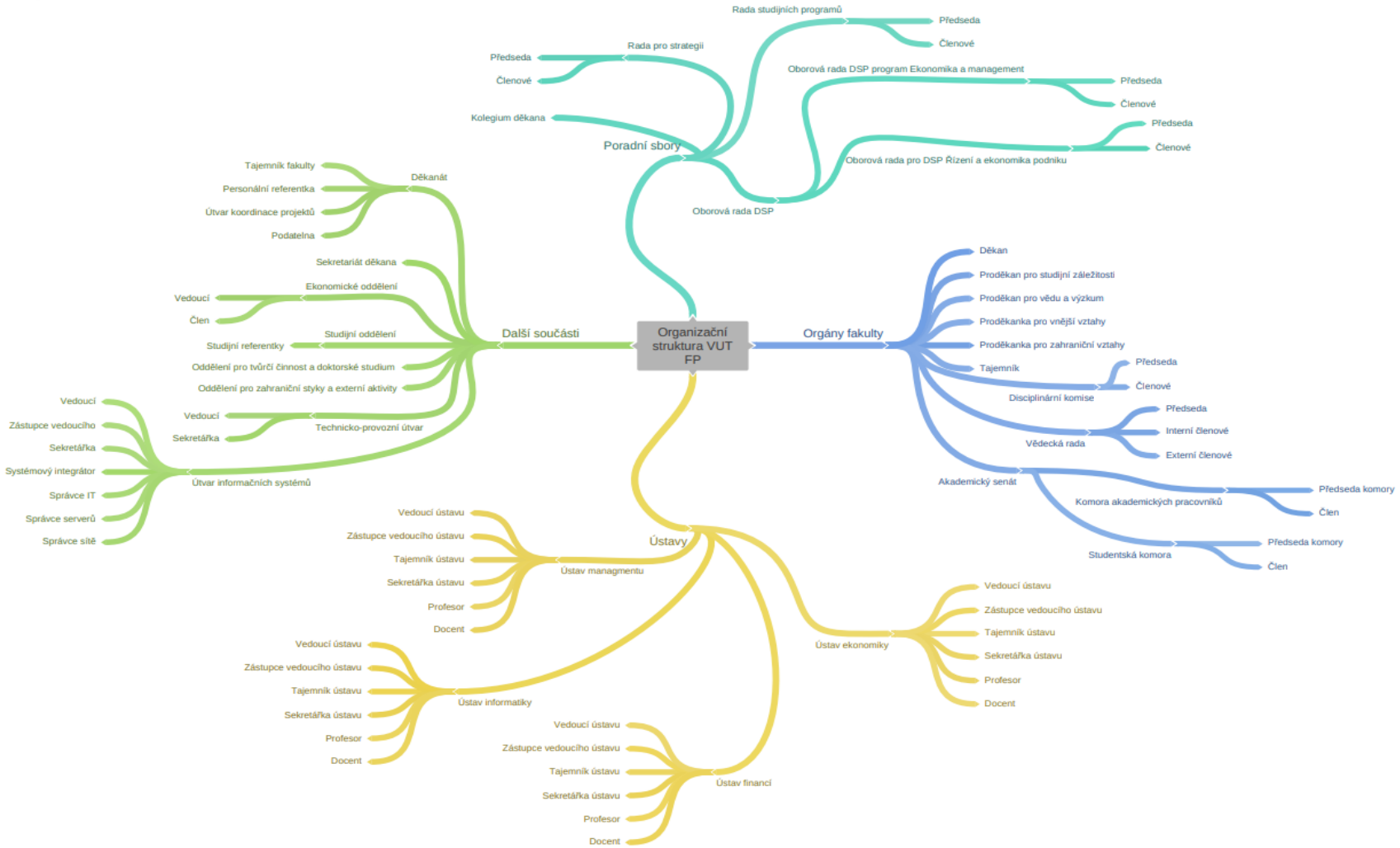
Následující kapitola obsahuje představení vybrané organizace, její organizační strukturu a zpracované analýzy, které byly představeny v teoretické části, na jejichž konci je celkové shrnutí analýz okolí. Na konci samotné analytické části se nachází ještě analýza rizik.

2.1 Představení organizace

Organizací, která byla vybrána pro zpracování diplomové práce, je Fakulta podnikatelská. Spadá pod VUT čili Vysoké učení technické a je situována v Brně v areálu Pod Palackého vrchem. Jde o nejmladší fakultu VUT. Fakulta podnikatelská vznikla z Katedry ekonomiky a řízení strojírenské výroby Fakulty strojní. K jejímu oficiálnímu vzniku došlo v září roku 1992 a necelý rok na to, v červnu 1993, došlo k zahájení její činnosti. Již v červenci roku 1994 proběhly na fakultě první promoce. V březnu roku 1996 došlo k otevření fakultní knihovny a studovny. Roku 1998 byly otevřeny dvě učebny pro výuku výpočetní techniky, a to k výročí oslav Dne studentů. Roku 2004 se fakulta přestěhovala do nového integrovaného objektu VUT, ve kterém působí dodnes (3). Fakulta se prezentuje tak, že je jejím posláním vychovat ekonomy a manažery v akreditovaných studijních programech. Studenti zde mohou získat bakalářský, magisterský nebo doktorský titul. Studentům je k dispozici navíc program celoživotního vzdělávání a programy MBA.

2.1.1 Organizační struktura

Pro jednodušší orientaci je organizační struktura předvedena v podobě myšlenkové mapy. Celá organizační struktura se dělí na 4 hlavní části, které se pak dělí dále, jak je v mapě vidět (5).



Obrázek 8: Organizační struktura VUT FP
(Zdroj: Vlastní zpracování dle 5)

2.2 SLEPTE

2.2.1 Sociální faktory

Hlavním sociálním faktorem, který má dopad a vliv na fakultu, je úbytek studentů. Všeobecně za posledních 5 let počty studentů vysokých škol klesaly, ačkoliv v roce 2019/2020 se oproti předchozímu roku číslo lehce zvedlo. Nicméně za poslední 3 roky se množství studentů pohybuje stále kolem 230 tis. (11). V roce 2018/2019 se na Fakultu podnikatelskou přihlásilo 3345 studentů, ze kterých bylo přijato 2101. Oproti tomu v roce 2019/2020 se přihlásilo 2954 studentů, což znamená pokles o 11,7 % oproti předchozímu roku, přijato jich bylo 2000, což je pokles o 4,8 % oproti roku 2018/2019.

Do letošního ročníku, tedy školního roku 2020/2021, se přihlásilo 2768 studentů, opět pokles o 6,3 % oproti předchozímu roku a oproti roku 2018/2019 dokonce pokles o 17,25 %. Z tohoto množství přihlášených studentů bylo přijato pouze 1647 studentů. To dělá pokles o 17,65 % oproti roku 2019/2020 a o 21,6 % méně studentů oproti roku 2018/2019 (12).

Zajímavé je, že ačkoliv čísla přihlášených a přijatých studentů klesají na některých fakultách VUT, na některých fakultách se čísla naopak za poslední tři roky zvyšují. Počty potenciálních studentů a přijatých studentů se zvyšují na Fakultě informačních technologií, což poukazuje na zvýšený zájem o práci v IT sféře, čísla se též zvedají na Fakultě architektury a Fakultě výtvarných umění. Na Fakultě elektrotechniky a komunikačních technologií, Fakultě chemické a Fakultě stavební čísla kolísají. Počty studentů pravidelně klesají pouze na Fakultě podnikatelské a Fakultě soudního inženýrství (13).

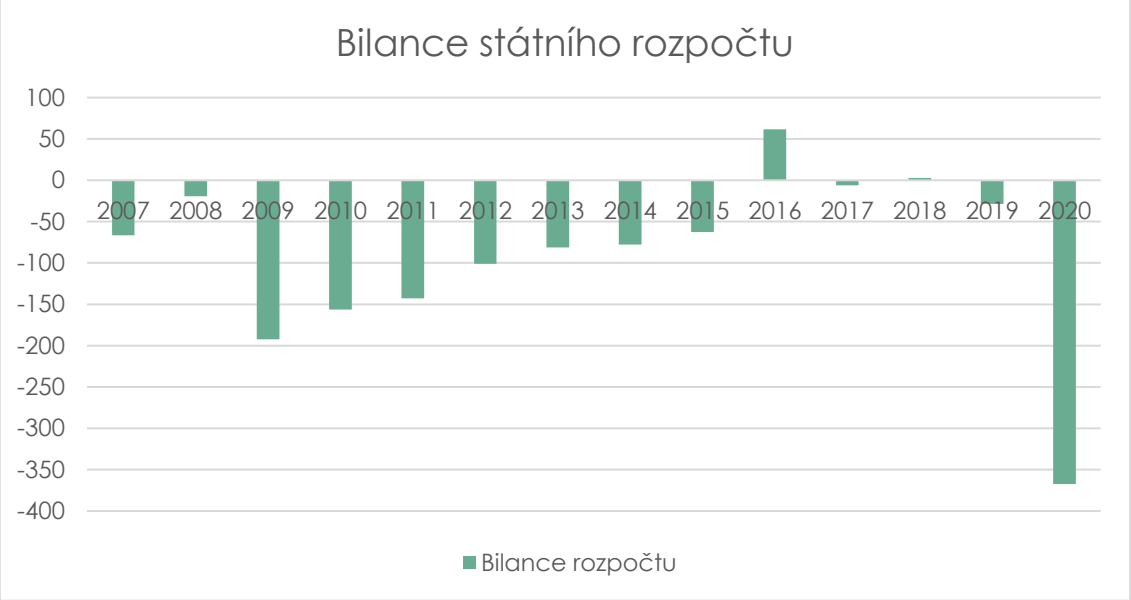
2.2.2 Legislativní faktory

Fakulta podnikatelská, jakožto veřejná vysoká škola, podléhá zákonům, vyhláškám a novelám zákonů. Pravděpodobně nejdůležitějším dokumentem, který je stěžejní a upravuje postavení vysokých škol v České republice, je zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění některých zákonů (zákon o vysokých školách). Tento zákon pojednává o základních informacích pro vysoké školy, jak se člení, jaké mají orgány, o akreditaci studijních programů a nevynechává podstatnou část, která je zaměřena na vztah s Ministerstvem školství, mládeže a tělovýchovy. Zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění některých zákonů (zákon o vysokých školách) samozřejmě není jediným zákonem, kterým se vysoké školy musí řídit. Existují

zákony, kterými jsou zřízeny jednotlivé vysoké školy a ve kterých lze nalézt konkrétnější specifikaci postavení dané vysoké školy. Lze nalézt i takové zákony, které upravují zvláštní pravidla pro vzdělávání, jak posuzovat dobu studia apod. (14). Samozřejmě se, kromě zmíněných zákonů, musí Fakulta podnikatelská řídit vládními nařízeními, vyhláškami a předpisy Ministerstva školství a bezpečností práce.

2.2.3 Ekonomické faktory

Nynější situace v České republice nevypadá vůbec příznivě. Pandemie viru COVID-19 negativně ovlivnila ekonomiky prakticky všech zemí světa a Česká republika není výjimkou. Příjmy státu klesají, nefunguje turismus, nejsou příjmy z obchodů a za služby, ale výdaje rostou. Celkové příjmy meziročně klesly o 5,4 %, ale výdaje se zvedly o 18,1 %. Došlo k propadu HDP a státního rozpočtu, což má vliv také na vysoké školy.



Obrázek 9: Bilance státního rozpočtu
(Zdroj: Vlastní zpracování dle 29)

Jak je na obrázku vidět, státní rozpočet se dokonce propadl hlouběji, než byl v ekonomické krizi v roce 2008. Nicméně vláda veřejné školy podporuje pomocí příspěvků a dotací, o které si školy mohou zažádat, jelikož stále musí platit své zaměstnance, výuka stále probíhá, přestože jen v distanční formě.

Vzhledem k tomu, že je Fakulta podnikatelská státním útvarem, platové ohodnocení zaměstnanců lze zjistit z tabulek. Plat vysokoškolského pedagoga se pohybuje v rozmezí zhruba 25 000 – 55 000 kč (16). O konkrétní výši pak rozhoduje dosažené vzdělání, praxe nebo region, ve kterém vyučuje.

VUT, potažmo i Fakulta podnikatelská, spolupracuje se zahraničními organizacemi a zahraničními vysokými školami, proto je důležité sledovat i směnný kurz eura ku koruně. Ke dni 30.3.2021 byl směnný kurz zhruba 26,1 Kč / 1 euro, ale ceny se samozřejmě lehce liší pro nákup a prodej. Na grafu níže lze vidět, jak se kurz v průběhu posledního roku vyvíjel. Kurz je dost kolísavý, zvlášť v druhé čtvrtině roku 2020, kdy v Evropě poprvé udeřila pandemie COVID-19. V létě euro lehce oslabilo, koruna posílila, ale ve druhé pandemické vlně na podzim roku 2020 euro opět posílilo. Zhruba od začátku roku 2021 je vidět lehká kolísavost kolem 26 Kč / 1 euro (17).

Obrázek 10: Graf vývoje kurzu euro/koruna
(zdroj: převzato z 17)

2.2.4 Politické faktory

Česká republika je zemí demokratickou a vláda je volena lidmi staršími 18 let. Nynější vláda byla volena v roce 2017, úřadu se chopila roku 2018 a jejím předsedou je Ing. Andrej Babiš. V rámci školství vláda slíbila zvyšování objemu financí, a to hlavně na platy pracovníků ve školství, omezení zbytečné a zdlouhavé byrokracie a mezi zásadní změny patří také úprava rámcových vzdělávacích programů. Jedná se hlavně o matematiku, jazykové vzdělávání a ICT. Vláda navíc přislíbila bezplatné vysokoškolské vzdělávání na státních a veřejných školách (19). Politické faktory jsou si s těmi legislativními celkem podobné. Vláda schvaluje novely, zákony a nařízení, a i na vládě

záleží, jaký finanční objem škola obdrží. Z těchto financí pak platí zaměstnance, veškerý svůj provoz.

Již prakticky od března roku 2020 (školní rok 2019/2020) je škola uzavřena (až na občasné uvolnění opatření) a pravděpodobně do konce školního roku 2020/2021 bude dostupná pouze distanční výuka. Toto opatření vydala vláda České republiky kvůli stávající pandemii COVID-19.

2.2.5 Technologické faktory

Díky technologickým faktorům může být organizace značně napřed oproti jí podobným, které ale technologické a technické novinky a pokrokům se nepřizpůsobují, případně je vůbec nesledují. Fakulta podnikatelská má k dispozici několik laboratoří výpočetní techniky, kde probíhají cvičení vybraných předmětů, ve většině učeben se nachází projektory pro zobrazení prezentací učiva a probírané látky (20).

2.2.6 Ekologické faktory

Jakožto každá fyzická či právnická osoba, tak i Fakulta podnikatelská se musí řídit zákony o odpadech a jak s ním nakládat. Prioritou je odpadu předcházet, nicméně pokud tak učinit nelze, tak existuje hierarchie, jak s odpadem nakládat. Na vrcholu hierarchie je příprava k opětovnému využití, pokud to nelze provést, na dalším stupni je recyklace. V případě, že ani recyklovat nelze, je potřeba pro odpad najít jiné využití (včetně energického využití). Není-li možné ani to, na spodu hierarchie se nachází odstranění odpadu. V České republice od roku 1.1.2021 je účinný zákon č. 541/2020 Sb., Zákon o odpadech. Jsou v něm sepsána práva a povinnosti všech osob, které figurují v odpadovém hospodářství a také popisuje základní principy oběhového hospodářství, ochranu životního prostředí a v neposlední řadě zdraví lidí při nakládání s odpady (21). Fakulta samotná poskytuje svým studentům dostatek odpadních košů na tříděný a smíšený odpad.

2.3 PORTER

2.3.1 Hrozba vstupu nových konkurentů – nízká

Většina univerzit v České republice vznikla ve 20. století, pokud nebereme v potaz ty nejstarší, jako je Karlova univerzita (14. století), Univerzita Palackého v Olomouci (16. století) a České vysoké učení technické (18. století). Vysoké učení technické nepatří k nejstarší, ale ani k nejmladším univerzitám v České republice. Založeno bylo v roce

1899 a dnešní název má od roku 1956, kdy došlo k přejmenování, původně se univerzita nazývala Česká technická vysoká škola v Brně (22). Fakulta podnikatelská je nejmladší fakultou VUT a byla založena roku 1992 (3). Jelikož je na trhu možnost velkého výběru vysokoškolského vzdělání, není nutné zakládat nové univerzity. Fakulta podnikatelská navíc nabízí takové obory, které nabízí i spousta jiných vysokých škol, případně jim podobné. Poptávka po ekonomických oborech je dostatečně nasycena a není nutné zakládat nové, proto je hrozba vstupu nových konkurentů nízká.

2.3.2 Hrozba stávajících konkurentů – velká

V Brně se nachází 10 vysokých škol, z toho je jich 5 veřejných, mezi které patří i VUT a jeho fakulty, 4 soukromé a 1 státní (23). Vysoké učení technické je prakticky jedinou vysokou školou, která se téměř výlučně zaměřuje na technické obory. Z toho vyplývá, že v Brně téměř nemá konkurenci, opět až na výjimky, například Fakultě informačních technologií VUT může konkurovat Fakulta informatiky MU. Nicméně pokud se ale bude brát v potaz celá Česká republika, tak konkurence Fakultě podnikatelské existuje. Fakult, které nabízí podobné obory jako nabízí Fakulta podnikatelská, je v České republice hned několik, takže studenti si mohou vybrat, kde budou chtít studovat (24). Mohou vybírat na základě reputace školy, doporučení a recenzí známých a lidí, co na dané škole studovali, na základě geografického umístění školy nebo třeba na základě pocitu, jak se škola jeví, jaké má webové stránky, jak vypadá a jak podporuje studenty.

Názory na Fakultu podnikatelskou se různí. Jakožto prakticky ekonomická fakulta nemá moc dobré jméno, respektive existují u nás lepší ekonomické fakulty. Říká se, že ekonomické obory na Fakultě podnikatelské jsou relativně jednoduché a pokud člověk studiu věnuje nějakou pozornost, neměl by být problém školu zvládnout (25). Fakulta nabízí ještě jeden obor, který je nejen čistě ekonomický, ale nabízí náhled i do IT.

Jelikož jsou na ekonomickou fakultu názory smíšené, ale všeobecné přesvědčení je takové, že jsou obory Fakulty podnikatelské brány za relativně lehce zvládnutelné, je hrozba stávajících konkurentů vysoká.

V rámci Brna jsou největšími konkurenty Masarykova univerzita, která má Ekonomicko-správní fakultu a Mendelova univerzita, která má Provozně ekonomickou fakultu. Obě nabízí ekonomické obory s podobným zaměřením, jako Fakulta podnikatelská. V rámci České republiky jsou konkurenty například Univerzita Karlova, jejíž Fakulta sociálních

studií nabízí také ekonomické obory nebo Univerzita Pardubice, která má svou Fakultu ekonomicko-správní.

2.3.3 Hrozba vzniku substitutů – nízká

Jak již bylo zmíněno výše, substituty již existují, jenom v Brně je zhruba 17 ekonomických škol a fakult, které nabízí ekonomické vzdělání, stejně jako Fakulta podnikatelská. Jsou brány v potaz školy veřejné i soukromé, studium, které lze skládat prezenčně i dálkově a typ studia (bakalářské, magisterské, doktorské) (26). Jelikož je trh s nabídkami ekonomického studia již nasycen, je hrozba vzniku nových substitutů nízká.

2.3.4 Vyjednávací síla zákazníků – střední

Zákazníci jsou v případě Fakulty podnikatelské studenti. Fakulta se snaží nabídnout nejen zajímavé předměty, poznatky a znalosti využitelné v praxi, ale klade důraz i na mimoškolní aktivity. Ročně se pořádá ples Fakulty podnikatelské, pro studenty prvních ročníků, a nejen pro ně, je k dispozici příručka studenta, která studenty prvních ročníků připraví na studium na vysoké škole, student může vycestovat na Erasmus a studovat semestr v zahraničí na spřátelených univerzitách. Fakulta podnikatelská nabízí možnost pracovních stáží v zahraničí, letních škol, přípravných kurzů na přijímací zkoušky a mnoho dalšího (27). Fakulta myslí i na budoucnost svých studentů, takže pravidelně hostuje Veletrh pracovních příležitostí, kde je spousta zástupců různých firem různého zaměření, kteří nabízí absolventům práci v oboru. Na veletrhu bývají desítky firem a veletrh je dostupný pro všechny studenty, nejen studenty z Fakulty podnikatelské. Letos, vzhledem k situaci, bude veletrh veden online formou (28).

Fakulta se snaží si studenty získat nejen svým přístupem ke studiu, nabídkou oborů a nabídkou mimoškolních aktivit, ale také starostí o kariérní postup studentů a hladký přechod studentů na pracovní pozice. Jak již dříve bylo zmíněno, konkurence je relativně vysoká, z toho plyne že ačkoliv fakulta nabízí spoustu zajímavých aktivit, pro spoustu studentů jistě atraktivních, riziko konkurence zde stále existuje, proto je vyjednávací síla studentů střední. Fakulta tak musí sledovat roční statistiky nejen své, ale i ostatních škol. Musí sledovat trendy, co studenty přiláká a podle toho se zařídit.

2.3.5 Vyjednávací síla dodavatelů – střední

Dodavateli Fakulty podnikatelské jsou nejen poskytovatelé energií, internetu, nábytku, pomůcek pro výuku (jako jsou počítače, prezentační plátna, projektory apod.), ale také například dodavatelé prodejních automatů, které mají k dispozici jak jídlo, tak i nápoje.

Při posuzování tohoto faktoru je potřeba vzít v potaz, k jakému účelu daný podnik zkoumáme a analyzujeme. Poskytovatelů elektřiny a plynu je na trhu celkem dost, nicméně v České republice je několik společností, které jsou tzv. tahouny, jsou nejčastěji využívané, jsou to firmy stabilní a jisté (jako například ČEZ, e-on). Ti budou mít vyjednávací sílu větší než zbývající, které tak často využívané nejsou. S poskytovateli internetu to je obdobné. Co se týče poskytovatelů nábytku, jako jsou lavice, pracovní stoly, vybavení učeben, tady je dodavatelů méně, na trhu se vyskytuje pár firem, které se zaměřují na vybavení pro školy (při zadání „Nábytek pro školy“ do vyhledávače bylo nalezeno asi 10 výsledků, které by přicházely v úvahu, ale většina všech výsledků vypadala jako firmy specializující se na nábytek pro základní a střední školy). Nedávno prošly některé přednáškové místnosti na Fakultě podnikatelské renovací. Takových dodavatelů, co zrenovují na zakázku učebnu a dodají nový nábytek, není mnoho, proto je jejich vyjednávací síla relativně vysoká. Naopak dodavatelů školních a pracovních pomůcek je hodně. V dnešní době existuje spousta technologických firem, které dodávají elektronické a technické pomůcky. Z toho plyne, že vyjednávací síla takových firem bude relativně nízká. Když se vezmou v potaz všechny zmíněné úrovně vyjednávacích sil, vychází to tak, že celková vyjednávací síla bude nabývat střední hodnoty.

2.4 7S

2.4.1 Strategie

Primárním cílem VUT je zajišťování kvality a strategického řízení. Škola se bude snažit nadále vytvářet vhodné prostředí pro možnost zapojení se všech pracovníků a pracovnic do řídících a rozhodovacích procesů. Bude sledovat okolní dění, vyhodnocovat vnější prostředí, bude posilovat pozici a společenskou roli univerzity. Aktuální strategický plán Fakulty podnikatelské pro rok 2021 nebyl zveřejněn, poslední zveřejněný plán je pro rok 2018, nicméně lze předpokládat, že záměry, cíle a strategie fakulty budou podobné. V roce 2018 byla prioritním cílem diverzita a dostupnost vzdělávací činnosti. Fakulta se zavázala k většímu začlenění odborníků z praxe do výuky, umožnit jim recenzování závěrečných prací, a dokonce je přizvat i do komisí k závěrečným zkouškám. Druhým prioritním cílem je stanovena internacionalizace. Pod tím je myšlena podpora jazykové vybavenosti pracovníků i studentů, podpora výuky předmětů v cizích jazycích, větší zapojení fakulty a jejích pracovníků v mezinárodních organizacích. Zavazuje se též ke

kvalitnímu a relevantnímu výzkumu, vývoji a inovacím. V neposlední řadě strategický plán obsahuje položku s efektivním hospodařením, kdy se zavazuje k zajištění financí na podporu inovací pro přizpůsobení obsahu i formy výuky nejnovějším trendům. Fakulta samozřejmě ve svém strategickém plánu neopomněla ani na lidské zdroje, kdy přislíbila větší podporu sebevzdělávání a seberozvoje pracovníkům a aktualizaci a vyhodnocení jejich plánu osobního rozvoje (30).

2.4.2 Styl řízení

Vzhledem k tomu, že přímo ve strategickém plánu Fakulty podnikatelské je bod, který říká, že se fakulta chce snažit o větší začlenění pracovníků a pracovnic do rozhodovacích a řídících procesů, bude zde převažovat demokratický styl řízení, jehož typickým znakem je větší participace pracovníků a delegace pravomocí. Záleží na tom, o jaké rozhodnutí se jedná. V některých případech bude převládat autoritativní styl řízení, kdy rozhoduje děkan, v některých případech je ale vhodnější zvolit demokratický styl řízení, kdy do rozhodnutí lze začlenit i ostatní pracovníky, kteří se na řešení budou podílet (31, s. 20).

2.4.3 Sdílené hodnoty

Pravděpodobně nejdůležitější položka na seznamu sdílených hodnot jsou vztahy na pracovišti. Neshoda s kolegou/kolegy, bývá hlavní příčinou výpovědí ze strany zaměstnanců. Z toho plyne, že nepsaným pravidlem je slušné chování ke kolegům, studentům a čestná reprezentace Fakulty podnikatelské. Všichni zaměstnanci se podílejí na hlavním cíli organizace, na její vizi, kterou je hlavně dostupnost vzdělání a diverzita (32).

2.4.4 Spolupracovníci

Zaměstnanci školy jsou nejen pedagogové, ale i externí pracovníci a nepedagogičtí pracovníci. Na konci každého školního roku vyhlašuje VUT možnost zvolit si nejlepšího pedagoga za bakalářské i magisterské studium. Vybírají se vítězové za každou fakultu za oba typy studií, kteří získají ocenění. Takové ocenění by mohlo být pro pedagogy motivující. Udržovat motivaci spolupracovníků je potřebné, proto VUT svým pracovníkům a kolegům nabízí možnosti kariérního růstu a různé motivační nástroje, které slouží jako odměny (32). Bylo by vhodná zavést větší spolupráci studentů a pedagogů ve formě například mimoškolních aktivit s pedagogy nebo třeba možnost spojit učivo s názornými ukázkami či exkurzemi do organizací.

2.4.5 Schopnosti

Jelikož si je VUT vědomé toho, že je potřeba se stále sebevzdělávat nabízí svým zaměstnancům vzdělávací kurzy, v době koronaviru je možné tyto kurzy absolvovat i distanční formou. Škola nabízí kurzy věnující se jak hard skills, jako je třeba práce se excelem, tak i na soft skills, jako například trénink paměti nebo třeba jak pracovat na home office a motivovat se. Vzhledem k zvýšenému výskytu syndormu vyhoření a jiných psychických nedostatků, nabízí VUT také kurzy psychologického poradenství (33). Samozřejmostí je možnost účasti na jazykových kurzech. Zaměstnancům jsou k dispozici kurzy angličtiny, němčiny, ruštiny, španělštiny, francouzštiny a italštiny, a to jak pro začátečníky, tak i pro pokročilé. Jazykové kurzy si jako jediné musí zaměstnanci zaplatit.

2.4.6 Systémy

Jak studenti, tak i zaměstnanci VUT mají k dispozici spoustu softwarových nástrojů, některé jsou založené na cloudovém řešení, některé jsou instalovatelné (34). Velkým problémem je absence povědomí o informační bezpečnosti a neexistující nástroj či software pro vysvětlení základů bezpečnosti na internetu či upevňování těchto základů. Byla by vhodná lepší správa webových stránek Fakulty podnikatelské, protože občas se na nich nenachází aktuální informace, a větší aktivita na sociálních sítích.

A) Instalovatelné

Některé softwarové nástroje jsou vyhrazeny pouze zaměstnancům, některé mohou používat i studenti a doktorandi. Nástroje jsou rozděleny do kategorií, kterými jsou výpočetní programy, kancelářské programy a antivirové programy. Z výpočetních programů mohou studenti i zaměstnanci využívat například Azure Dev Tools (dostupné taky jako cloudové řešení) nebo například nově MATLAB (dostupné i jako cloudové služba). V rámci kancelářských programů lze využít Sketch Engine nebo ASPI (Automatizovaný systém právních informací). K antivirovým programům studenti bohužel přístup nemají, tato nabídka je dostupná pouze zaměstnancům (35).

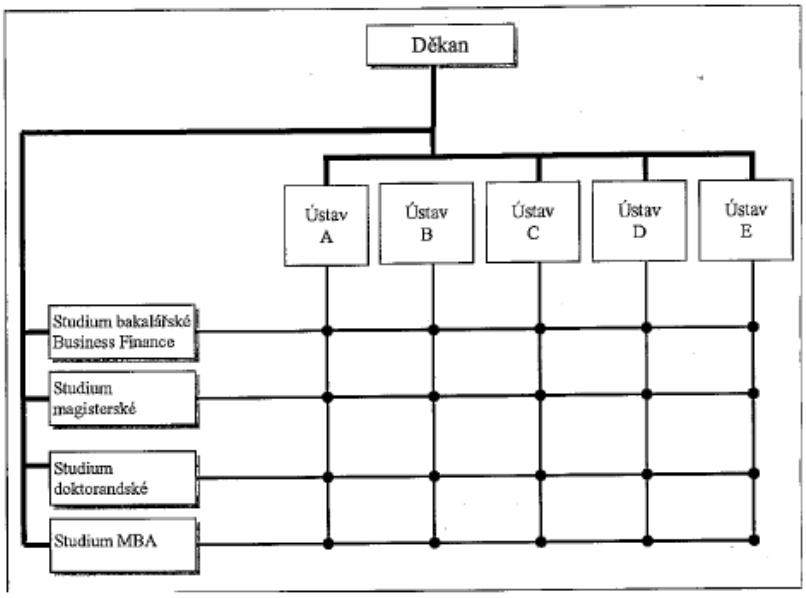
Jakožto ekonomický software VUT využívá SAP, který spolupracuje s Komerční bankou (KB) a Československou obchodní bankou (ČSOB). Aplikace, pomocí které se zaměstnanci mohou přihlašovat do SAPu se dá stáhnout jak pro operační systém Windows (7 a 10), tak i pro macOS. Lze využít i software OpenText pro skenování faktur do SAPu (36).

B) Cloudové služby

Studenti i zaměstnanci se mohou přihlašovat pomocí přihlašovacích účtů a hesel do cloudových služeb Google a Microsoft. VUT poskytuje licence Microsoft 365, kam spadá Word, Excel, Outlook, PowerPoint, OneNote. Pro studenty je navíc k dispozici Publisher a Access. Lze využít i licenci pro Power BI a Project Plan 5. Aplikace je možné si nainstalovat až na 5 zařízení. V neposlední řadě lze cloudově využít i MATLAB a Azure DevTools (37).

2.4.7 Struktura

Fakulta podnikatelská spadá do maticové organizační struktury i přes to, že je to struktura typická pro výrobu. Každý pracovník má své dva nadřízené, a to odborného vedoucího a vedoucího týmu. Je potřeba, aby pracovník odevzdával výsledky své práce, případně je hlásil, oběma nadřízeným. V týmech se vyskytuje několik pracovníků z různých ústavů a všichni se podílí na řešení úkolů (31, s. 17). Strukturu lze lépe vystihnout obrázkem.



Obrázek 11: Maticová struktura fakulty vysoké školy
(zdroj: převzato z 2, s. 18)

2.5 SWOT

Obrázek 12: SWOT analýza Fakulty podnikatelské
(zdroj: Vlastní zpracování)

Jak už bylo zmíněno v kapitole 1.13, tak tato analýza pokládá do protikladu faktory SW a OT, které mezi sebou můžeme vzájemně porovnávat a podle výsledků následně vyhodnotit. Vychází z analýzy 7S, SLEPTE i z analýzy Porter. Je nutné se zaměřit na nedostatečné vzdělání studentů a školení zaměstnanců v oblasti informační bezpečnosti, která je stále palčivějším tématem. Proto se tomuto problému bude věnovat návrhová část.

2.6 Souhrn analýz

Byly provedeny celkem 4 analýzy vnějšího a vnitřního prostředí organizace. Analýza SLEPTE je analýzou obecného okolí neboli vnějšího prostředí. Ta pomáhá pochopit vnější vlivy, které na organizaci působí, nelze je ovlivnit, ale je potřeba s nimi počítat a sledovat je. Jedná se o faktory sociální, legislativní, ekonomické, politické, technologické a ekologické. Byly rozebírány snižující se počty přihlášených a přijatých studentů

(sociální), nutnost fakulty dodržovat zákon o vysokých školách a zákony a vyhlášky s tím spojené (legislativní). Na přetřes přišly i ekonomické dopady pandemie, změny peněžních kurzů (ekonomické) a uzavření škol kvůli vládnímu nařízení (politické). Bylo zmíněno technologické vybavení fakulty (technické) a analýza byla zakončena zmínkou o způsobech, jakým FP nakládá s odpady (ekologické).

Druhou provedenou analýzou byla analýza oborového okolí, analýza konkurenceschopnosti. Jedná se Porterův model 5 konkurenčních sil. Každá síla byla podrobně popsána a bylo připojeno i slovní hodnocení této síly. Vzhledem k náročnosti vstupu na trh je hrozba vstupu nových konkurentů ohodnocená jako nízká. Nová vysoká škola pravděpodobně brzo vznikat nebude a vznik nové fakulty na již existující škole, případně vznik nového oboru, který by poskytoval podobně zaměřené vzdělání jako FP, je též nepravděpodobný, protože školy s dobrým hodnocením a reputací již podobné obory mají v nabídce. Z toho plyne, že hrozba stávajících konkurentů je vysoká. Jak již bylo zmíněno, substituty existují, proto je hrozba vzniku nového substitutu nízká. Posledními faktory jsou vyjednávací síly zákazníků a dodavatelů, které jsou ohodnocené jako střední, a to z toho důvodu, že záleží na úhlu, z jakého se na problematiku nahlíží. V některých případech bude vyjednávací síla vysoká u obou faktorů, v jiných případech může být nízká, proto jsou tyto dva faktory ohodnoceny jako střední síla.

Předposlední analýzou, která byla provedena, je analýza interních faktorů neboli analýza 7S. Tato analýza zkoumá sedm faktorů, kterými jsou strategie, styl řízení, sdílené hodnoty, spolupracovníci, schopnosti, systémy a struktura organizace.

Poslední analýzou, která je v této práci využita, je analýza SWOT. Ta zkoumá silné a slabé stránky, které vychází z analýzy 7S, a příležitosti a hrozby, které vychází z analýz SLEPTE a Porter.

2.7 Analýza rizik

Je nezbytné o rizicích vědět, znát je, uvědomit si, co mohou způsobit a vytvořit si ke každému významnějšímu riziku protiopatření, kterým by se dalo riziko eliminovat, nebo aspoň snížit jeho dopad. Analýza rizik se skládá z několika kroků, které představují

následující kapitoly. Nejdříve bude provedena identifikace rizik, následně tato rizika budou ohodnocena, čímž se získá jejich úroveň. V následující kapitole budou tyto úrovně zobrazeny v přehledné mapě rizik. Poslední část analýzy rizik je sestavení protiopatření vůči rizikům s nejvyššími hodnotami.

2.7.1 Identifikace a ohodnocení hrozeb

Prvním krokem je stanovení si hrozeb, jejich identifikace. Druhým krokem je nezbytné ohodnocení hrozeb. Pro potřeby této diplomové práce byla zvolena kvalitativní metoda analýzy kvůli její snadné interpretaci. Bude stanovena hodnota rizika vzniku dané hrozby, následovaná jejím ohodnocením dopadu na projekt. Tyto údaje budou číselně vyjádřeny hodnotami od 1 do 10, přičemž 1 znamená nejmenší riziko nebo dopad, 10 je nejvyšší. Analýza bude provedena tzv. skórovací metodou. Výslednou hodnotu hrozby zjistíme vzájemným vynásobením hodnoty rizika a dopadu.

Tabulka 1: Identifikace a ohodnocení rizika
(Zdroj: Vlastní zpracování)

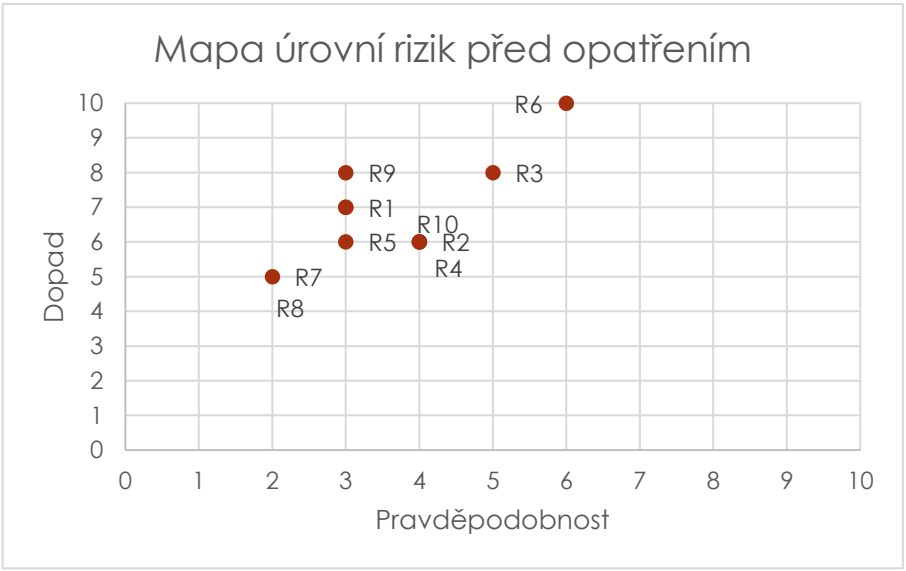
Pořadí hrozby	Hrozba	Riziko	Dopad	Úroveň rizika
R1	Nedostatečné školení	1	7	7
R2	Malá informovanost o školení	2	6	12
R3	Špatným způsobem zpracovaná metodika	5	8	40
R4	Překročení finančního plánu	5	6	30
R5	Nedodržení časového plánu	3	6	18
R6	Ztráta dat	2	10	20
R7	Nevhodná komunikace plánu s cílovými skupinami	2	5	10
R8	Chybný postup při zavádění	3	7	21
R9	Vysoká náročnost pro uživatele	1	8	8
R10	Vysoký zájem, nebudou postačovat kapacity	6	6	36

2.7.2 Mapa rizik

Mapa rizik přehledně zobrazuje možnost výskytu a dopad. Pro správné pochopení mapy rizik a hlavně toho, co z této mapy lze vyvodit, je ještě potřeba rozdělit si mapu na 4 kvadranty podle důležitosti rizika.

Obrázek 13: Kvadranty mapy rizik podle skórovací metody
(Zdroj: Převzato z 38, s. 96)

Kvadrant bezvýznamných hodnot rizik obsahuje hrozby s nejnižšími hodnotami pravděpodobnosti a dopadu, tato rizika není nutné ošetřovat. Do kvadrantu běžných hodnot rizik spadají hrozby, které mají vyšší pravděpodobnost vzniku, ale nízký dopad, proto je vhodné je sledovat, ale není potřeba akutně zasahovat a hrozby ošetřovat. Už z názvu kvadrantu významných hodnot rizik plyne, že se jedná o hrozby, které je potřeba nejen sledovat, ale mít pro ně připravené i protiopatření. Poslední kvadrant kritických hodnot rizik obsahuje hrozby, které mají jak vysokou pravděpodobnost, tak i vysoký dopad a je nezbytné je ošetřit, aby se snížila úroveň rizika.



Obrázek 14: Mapa úrovní rizik před opatřením
(Zdroj: Vlastní zpracování)

Jak je v mapě úrovní rizik vidět, většina hrozeb spadá do kvadrantu významných hodnot rizik. To znamená, že těmto hrozbám by měly vzniknout protiopatření. Jedna hrozba, a sice R10, spadá do kvadrantu kritických hodnot rizik, tady je nezbytné ji v ideálním případě eliminovat, nebo aspoň snížit její úroveň rizika. Pouze R7 spadá do kvadrantu bezvýznamných hodnot rizik. Tato hrozba má jak nízké riziko, tak relativně nízký dopad. Je ale potřeba podotknout, že hrozba je na hranici s kvadrantem významných hodnot rizik.

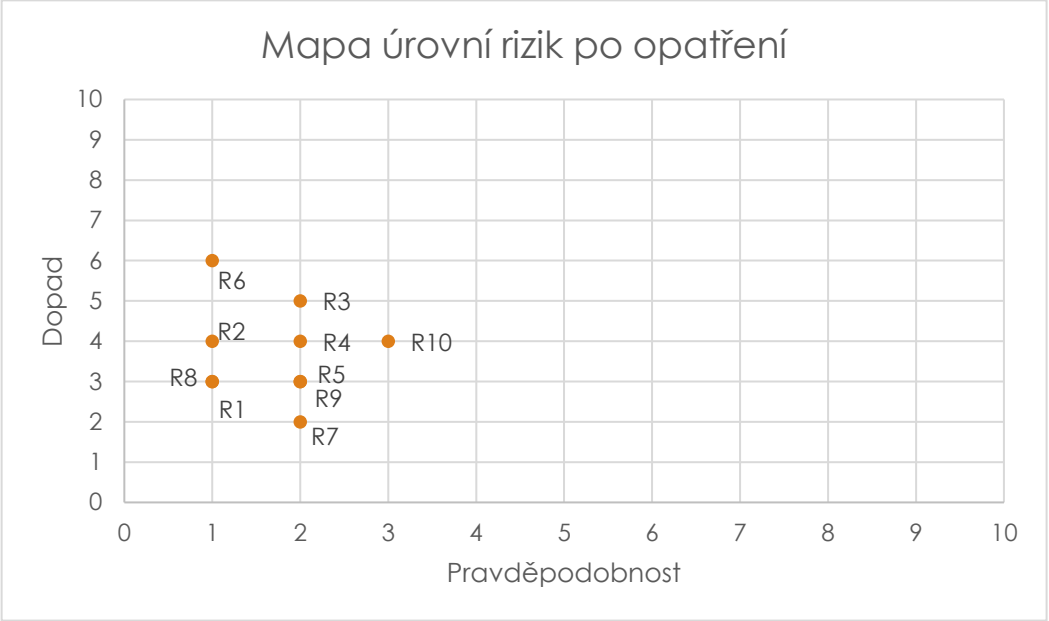
2.7.3 Opatření hrozeb

Je vhodné se při vytváření protiopatření vůči hrozbám řídit mapou rizik, protože není nutné, a prakticky není ani možné, vytvářet protiopatření pro všechny hrozby. Ty, které mají nízkou hodnotou lze akceptovat, protože je nízké riziko, že vznikne, nebo by byl naprosto zanedbatelný dopad dané hrozby. Jak je vidět v mapě rizik, téměř všem hrozbám je potřeba vytvořit protiopatření. To znamená, že je potřeba snížit jejich úroveň zavedením takových opatření, která by snížila dopad hrozby, její riziko nebo by hrozbu úplně eliminovalo. Pouze hrozba R7, což je nevhodná komunikace s cílovými skupinami, lze přijmout, protože spadá do kvadrátu bezvýznamných hodnot rizik. Ale jelikož je na hranici, je v následující tabulce zahrnuta také s tím, že bude potřeba ji sledovat a v průběhu zavádění změny vyhodnocovat, zda se zvyšuje riziko či dopad a případně využít protiopatření.

Tabulka 2: Protiopatření na snížení hodnoty rizika
(Zdroj: Vlastní zpracování)

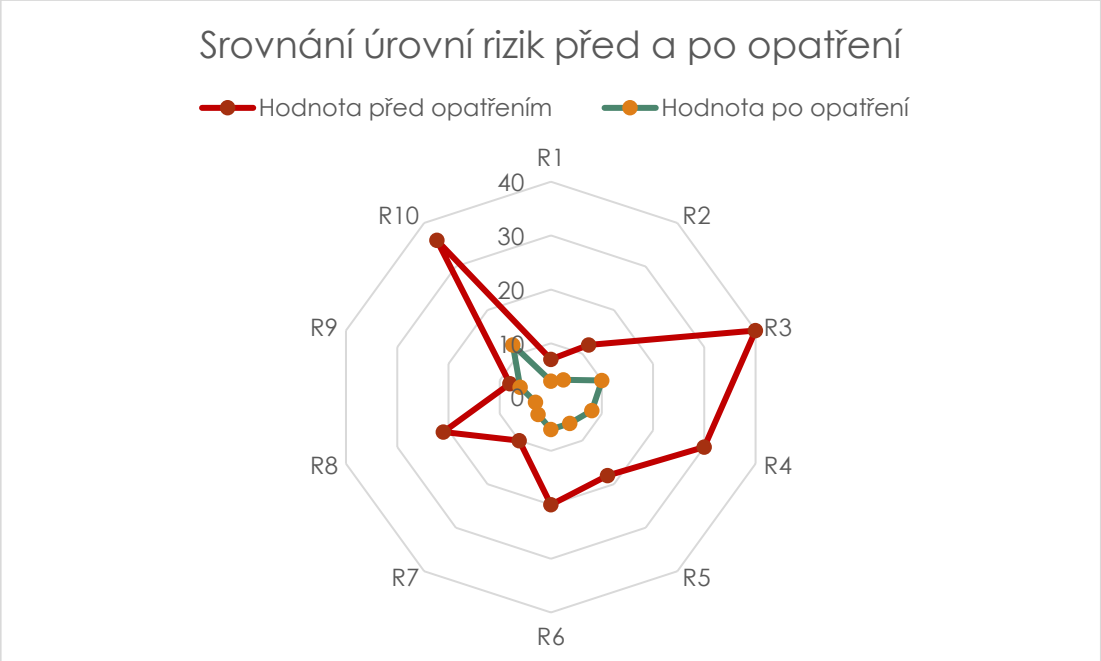
Hrozba	Protiopatření	Riziko	Dopad	Úroveň rizika
R1	Na konci školení prověřit znalosti školených, případně přidat více školení, doškolit.	1	3	3
R2	Zvýšení množství informačních letáčků, informační emaily pro zaměstnance i studenty.	1	4	4
R3	Důsledná příprava při zpracování, průběžná kontrola, konzultace s odborníky.	2	5	10
R4	Průběžné sledování rozpočtu, rozpočet plánovaný s nějakou rezervou.	2	4	8
R5	Stanovení si milníků, při kterých se bude kontrolovat, zda není projekt opožděn.	2	3	6
R6	Pravidelná záloha dat.	1	6	6
R7	Předem si udělat dotazníkový průzkum, jakým způsobem by školeným nejvíce vyhovoval způsob komunikace.	2	2	4
R8	Pečlivé naplánování předem, v průběhu zavádění kontrola reality s plánem.	1	3	3
R9	Zajištění, aby byly podklady pro školení uživatelsky jednoduché.	2	3	6
R10	Zavedení rezervačního systému na konkrétní data pro školení zaměstnanců.	3	4	12

Mapa úrovní ošetřených úrovní rizik



Obrázek 15: Mapa úrovní rizik po opatřeních
(Zdroj: Vlastní zpracování)

Jak je na nové mapě úrovní rizik vidět, podařilo se rizika i dopad hrozeb snížit pomocí protiopatření. Téměř všechny hrozby se podařilo přesunout do kvadrantu bezvýznamných hodnot rizik. Pouze hrozba R6 je v kvadrantu významných hodnot rizik, a to z toho důvodu, že i přes snížení jak rizika, tak i dopadu, je dopad stále relativně vysoký.



Obrázek 16: Srovnání úrovní rizik
(Zdroj: Vlastní zpracování)

Na mapě, která srovnává úrovně rizik před a po opatřeních, je přehledně vidět, že úrovně se po opatření podstatně snížily, většina jich je v takovém stavu, který pouze monitorujeme, ale akceptujeme jej.

3 Vlastní návrhy řešení

V první řadě se tato diplomová práce zabývá budováním bezpečnostního povědomí na fakultě podnikatelské. V první části kapitoly se nachází Lewinův model s jehož pomocí bude stanoveno, zda se plánovaná změna má aplikovat či nikoliv a bude stanoven seznam činností, které je potřeba v rámci provádění změny vykonat. Následuje časová analýza, která přehledně zobrazí trvání projektu a rizikové činnosti, které se nesmí zpozdit, aby nedošlo k prodloužení trvání projektu. Dalšími kapitolami jsou cíl a budování strategie a plánu SAE programu. Budou určeny klíčové role a jejich odpovědnosti, cíle, kterých má být v rámci každé úrovně SAE programu dosaženo a jak často cyklus učení opakovat, aby došlo k zapamatování jeho obsahu. Důležitou částí návrhové části je zpracování, rozvoj a šíření materiálů pro zvyšování povědomí. Návrhová část je zakončena finančním zhodnocením a post-implementační fází, která obsahuje způsoby zpětné vazby.

3.1 Lewinův model

Jak již bylo zmíněno v teoretické části, Lewinův model se skládá ze tří fází, kterými jsou fáze rozmrazení, fáze přechodu a aplikace změny a fáze zmrazení. Jednotlivé fáze budou dále podrobněji vysvětleny a objasněny.

3.1.1 Fáze rozmrazení

Nejdřív dojde k analýze silového pole pro zjištění, zda změnu aplikovat či nikoliv. Analýza je následována stanovením intervenčních oblastí s popisem, zda se jich změna dotkne či nikoliv. Na konci fáze rozmrazení budou určeni nositelé změny, mezi které patří agent změny, sponzor změny a advokát změny.

Analýza silového pole

Níže jsou v tabulkách vypsány síly, které působí na změnu, a to ať už se jedná o kladné, nebo záporné působení. Každá síla je ohodnocená od 1 do 5 podle toho, jaký vliv na změnu mají, přičemž 5 = velký vliv, 1 = malý až zanedbatelný vliv.

Tabulka 3: Síly působící pro změnu
(Zdroj: Vlastní zpracování)

Síly působící pro změnu	Hodnocení
Vedení školy	5
Zaměstnanci školy	4
Lepší reputace školy	4
Ministerstvo školství	2
Větší informační bezpečnost	4
Celkem	**19**

Tabulka 4: Síly působící proti změně
(Zdroj: Vlastní zpracování)

Síly působící proti změně	Hodnocení
Finanční výdaje navíc	4
Časová náročnost	3
Nutné zaškolení pedagogů	2
Celkem	**9**

Jak lze výše vidět, tak hodnota sil, které působí pro změnu je vyšší než výsledný součet hodnocení sil proti změně. Z toho plyne, že výsledek analýzy silového pole je kladný čili je možné změnu realizovat.

Intervenční oblasti

- Lidské zdroje a jejich řízení – Za vytvoření bude zodpovídat již existující a fungující oddělení VUT, tudíž nebude potřeba najímat externí firmu či nové pracovníky, aby změnu zavedli. Bude najata externí firma pouze pro vykonání školení a bude vést též vzdělávání.
- Organizační struktura firmy – Ani organizační strukturu provedení změny a její fungování nijak nepostihne.
- Technologie firmy – Dojde ke zlepšení bezpečnosti jak soukromých dat studentů i zaměstnanců, tak i stávajícího softwaru.
- Komunikační a organizační toky a procesy firmy – Díky školením bude komunikace lépe zabezpečena, zaměstnanci fakulty budou znát základy

informační bezpečnosti a pro případné narušitele tak bude těžší zjistit a zneužít přihlašovací údaje zaměstnance.

Nositel změny

- Agent změny – V případě Fakulty podnikatelské je agentem změny Útvar informačních systémů.
- Sponzor změny – Jelikož se jedná o fakultní záležitost, tak sponzorem změny bude Fakulta podnikatelská. Ta bude zodpovědná za dodání potřebných materiálů, jako jsou například informační letáčky, musí poskytnout lidské zdroje a samozřejmě zdroje finanční.
- Advokát změny – Tím jsou všichni studenti, pro které budou připraveny informační letáčky, workshopy apod., advokátem změny jsou ale i zaměstnanci, kteří budou pravidelně absolvovat odborná školení.

3.1.2 Fáze přechodu a aplikace změny

Tato fáze je pravděpodobně nejdůležitější. V této fázi probíhá samotná změna a budou v ní určeny činnosti, které je ke změně potřeba učinit. Následující tabulka obsahuje popisy činností, ke kterým je přiděleno vždy odpovídající písmeno pro lepší orientaci.

Realizace změny

Tabulka 5: Seznam činností
(Zdroj: Vlastní zpracování)

Činnost	Popis činnosti
A	Analýza stávajícího stavu
B	Určení rozsahu změny
C	Analýza uživatelů
D	Rozdělení uživatelů do cílových skupin
E	Určení rolí a zodpovědností
F	Stanovení cílů pro cílové skupiny
G	Komunikace plánu s cílovými skupinami
H	Stanovení struktury SAE
I	Vytvoření směrnic a politik
J	Zpracování metodiky pro každou cílovou skupinu
K	Vytvoření výukových materiálů pro každou skupinu uživatelů
L	Vytvoření časového harmonogramu školení
M	Vytvoření doprovodné dokumentace pro všechny skupiny (prezenční listiny, důkazy o školení apod.)
N	Školení cílových skupin
O	Vytvoření post-implementační dokumentace
P	Vyhodnocení a zpětná vazba
Q	Stanovení harmonogramu aktualizace výukových materiálů
R	Kalkulace
S	Sledování dodržování a efektivity
T	Vyhodnocení projektu

3.1.3 Fáze zmrazení

Fáze, která má svou důležitost a nesmí se na ni zapomínat. V této fázi už je změna hotová, nové postupy, směrnice a politiky jsou již novým standardem. Zhodnotí se změna, její průběh a její dopad. Hodnotí se dosažené výsledky, které mohou nabývat nejen slovního hodnocení (např. zpětná vazba od cílových skupin), ale mohou být vyjádřeny i číselně (např. procentuální snížení počtu úspěšných kybernetických útoků na organizaci). Probíhá verifikace, zda byli zaměstnanci a studenti správně proškoleni a jaký mělo

školení přínos. Výsledkem by měl být větší přehled o informační bezpečnosti, informovanost o tom, jak nakládat nejen se svými osobními údaji, ale i s citlivými informacemi organizace.

3.2 Časová analýza

Tato kapitola je věnována sestavení časové analýzy pomocí metody PERT. Nejdříve budou stanoveny optimistické, pesimistické a realistické doby trvání jednotlivých činností, které byly sepsány již v kapitole 3.1.2 Fáze přechodu a aplikace změny.

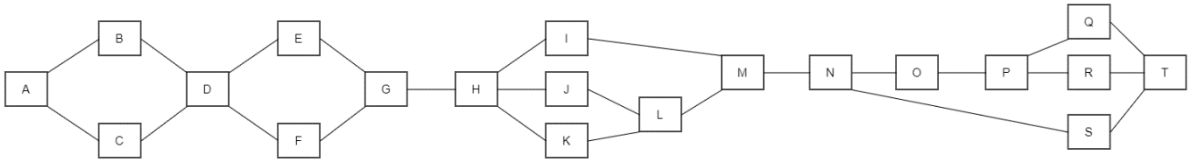
3.2.1 Metoda PERT

Tabulka 6: Návaznost činností s odhadem doby trvání
(Zdroj: Vlastní zpracování)

Činnost	Navazující činnost	Optimistický odhad	Realistický odhad	Pesimistický odhad
A	B, C	20	30	45
B	D	7	13	20
C	D	3	8	10
D	E, F	2	4	7
E	G	3	6	9
F	G	6	10	15
G	H	7	16	21
H	I, J, K	25	32	50
I	M	40	58	75
J	L	10	20	38
K	L	15	27	40
L	M	5	8	14
M	N	4	11	16
N	O, S	20	30	45
O	P	8	14	22
P	Q, R	9	15	25
Q	T	7	9	15
R	T	5	8	16
S	T	30	49	60
T	-	3	6	8

3.2.2 Grafické zpracování návaznosti činností

Pro lepší přehlednost návaznosti činností slouží následující obrázek.



Obrázek 17: Návaznost činností
(Zdroj: Vlastní zpracování)

3.2.3 Časová analýza

V této kapitole budou vysvětleny zkratky, které jsou použity v tabulce v následující kapitole, a jejich výpočet.

Tabulka 7: Vysvětlivky pro tabulku pro určení kritické cesty metodou PERT
(Zdroj: Vlastní zpracování)

Název	**Zkratka**
Předcházející činnost	i
Následující činnost	j
Optimistický odhad trvání činnosti	a_{ij}
Pesimistický odhad trvání činnosti	b_{ij}
Realistický odhad trvání činnosti	m
Deterministický model	t(ij)
Rozptyl	$\sigma^2 = \frac{(b_{ij} - a_{ij})^2}{36}$
Směrodatná odchylka	$\sigma = \frac{(b_{ij} - a_{ij})}{36}$
Začátek možný	ZM = KM předcházející činnosti (pokud je jich více, bere se větší číslo)
Konec možný	KM = ZM + t(ij)
Začátek přípustný	ZP = KP – t(ij)
Konec přípustný	KP = ZP následující činnosti (pokud je jich více, bere se menší číslo)
Rezerva celková	RC = KP – KM nebo RC = ZP – ZM (výsledky musí vyjít shodně). Nulové činnosti tvoří kritickou cestu.

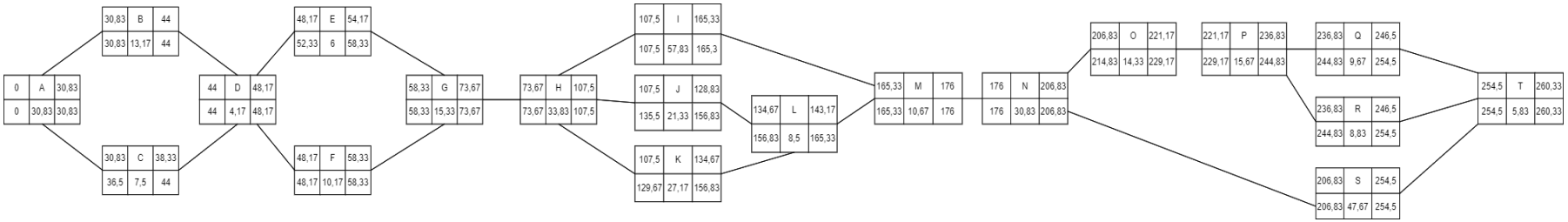
Kritická cesta – Cesta složená z činností s nulovou rezervou. Činnosti na této cestě se nesmí zpozdit, jinak se zpozdí celý projekt. Tyto činnosti nemají žádnou časovou rezervu a musí se stihnout v termínu. Kritická cesta je nejdelší cestou v grafu.

3.2.4 Určení kritické cesty

Tabulka 8: Výpočet kritické cesty pomocí metody PERT
(Zdroj: Vlastní zpracování)

Údaje o postupnosti činností projektu			Trvání (dny)				Statistické ukazatele		Termíny zahájení a ukončení činností				Rezerva
Činnost	i	j	a_{ij}	b_{ij}	m	t(ij)	σ2	σ	ZM	KM	ZP	KP	RC
A		B, C	20	45	30	30,83	17,36	4,17	0	30,83	0,00	30,83	0,00
B	A	D	7	20	13	13,17	4,69	2,17	30,83	44,00	30,83	44,00	0,00
C	A	D	3	10	8	7,50	1,36	1,17	30,83	38,33	36,50	44,00	5,67
D	B, C	E, F	2	7	4	4,17	0,69	0,83	44,00	48,17	44,00	48,17	0,00
E	D	G	3	9	6	6,00	1,00	1,00	48,17	54,17	52,33	58,33	4,17
F	D	G	6	15	10	10,17	2,25	1,50	48,17	58,33	48,17	58,33	0,00
G	E, F	H	7	21	16	15,33	5,44	2,33	58,33	73,67	58,33	73,67	0,00
H	G	I, J, K	25	50	32	33,83	17,36	4,17	73,67	107,50	73,67	107,50	0,00
I	H	M	40	75	58	57,83	34,03	5,83	107,50	165,33	107,50	165,33	0,00
J	H	L	10	38	20	21,33	21,78	4,67	107,50	128,83	135,50	156,83	28,00
K	H	L	15	40	27	27,17	17,36	4,17	107,50	134,67	129,67	156,83	22,17
L	J, K	M	5	14	8	8,50	2,25	1,50	134,67	143,17	156,83	165,33	22,17
M	I, L	N	4	16	11	10,67	4,00	2,00	165,33	176,00	165,33	176,00	0,00
N	M	O, S	20	45	30	30,83	17,36	4,17	176,00	206,83	176,00	206,83	0,00
O	N	P	8	22	14	14,33	5,44	2,33	206,83	221,17	214,83	229,17	8,00
P	O	Q, R	9	25	15	15,67	7,11	2,67	221,17	236,83	229,17	244,83	8,00
Q	P	T	7	15	9	9,67	1,78	1,33	236,83	246,50	244,83	254,50	8,00
R	P	T	5	16	8	8,83	3,36	1,83	236,83	245,67	245,67	254,50	8,83
S	N	T	30	60	49	47,67	25,00	5,00	206,83	254,50	206,83	254,50	0,00
T	S, R, Q		3	8	6	5,83	0,69	0,83	254,50	260,33	254,50	260,33	0,00

3.2.5 Síťový graf



Obrázek 18: Síťový graf
(Zdroj: Vlastní zpracování)

Síťový graf je přehlednější zobrazení tabulky z předchozí kapitoly. Jedná se o uzlově orientovaný graf, což znamená, že uzly představují činnosti A-T, které je potřeba pro vykonání změny udělat.

3.2.6 Popis uzlu

Každý uzel vypadá následovně:

ZM	OA	KM
ZP	t(ij)	KP

Obrázek 19: Popis uzlu ze síťového grafu
(Zdroj: Vlastní zpracování)

OA = označení činnosti, kterou uzel představuje

Zvýrazněné buňky v tabulce v předchozí kapitole označují kritickou cestu., kterou tvoří uzly: A-B-D-F-G-H-I-M-N-S-T.

3.3 Cíl SAE

Primárním cílem programu SAE je ochrana dat, informací a aktiv organizace. V rámci této diplomové práce bude zpracována pouze část programu, jelikož odborné přednášky a kurzy pro úrovně školení a vzdělávání povede externí firma. Vybraná firma bude moci školeným pracovníkům zaměstnancům vystavit certifikát o školení a o dosažení dané úrovně, což by Fakulta podnikatelská udělat nemohla. Externí firma byla vybrána také kvůli nedostatku odborníků na fakultě.

3.4 Stanovení strategie a plánu SAE

Obsahem této podkapitoly je stanovení strategie programu SAE. To zahrnuje stanovení rolí a odpovědností, stanovení cílů, kterých má být pro každou úroveň dosaženo (povědomí, školení, vzdělávání a profesní rozvoj) a způsobů zpětné vazby.

3.4.1 Odpovědnosti a role

Jak již bylo zmíněno v kapitole 1.4.5, v rámci SAE programu je definováno pět rolí, kterými jsou vedení organizace, CIO, CISO, manažeři a uživatelé. Je nezbytné si určit představitele těchto rolí, včetně stanovení si jejich odpovědností.

Tabulka 9: Rámec bezpečnostního povědomí na Fakultě podnikatelské
(Zdroj: Vlastní zpracování)

	Povědomí	Školení	Vzdělávání	Profesní rozvoj
Vedení fakulty	X	X	X	
Zaměstnanci	X	X		
IT zaměstnanci	X	X	X	
Správce sítě	X	X	X	X
Technicko-provozní útvar	X			
Studenti	X			
Studenti IM	X	X	X	

Vedení fakulty – děkan, proděkani

Zaměstnanci – tajemník, akademický senát, vědecká rada, disciplinární komise, sekretariát, studijní oddělení, ekonomické oddělení, zahraniční referentky, externí zaměstnanci

IT zaměstnanci – pracovníci IT oddělení

Správce sítě – vedoucí útvaru IS

Technicko-provozní útvar – údržba

Rozdělení rolí a odpovědností

- **Vedení organizace**

První rolí v seznamu je vedení organizace, které sestává z děkana a proděkanů. Jak už bylo zmíněno dříve v teoretické části, tak vedení má za úkol stanovit CIO, přidělit odpovědnost pracovníkům IT bezpečnosti, ujistit se, že se v organizaci vyskytují zaměstnanci, kteří mají potřebné znalosti a zkušenosti, které jim pomohou v ochraně informačních zdrojů. V neposlední řadě bude mít vedení univerzity na starosti prověřit, že plánovaný program SAE zahrnuje všechny potřebné oblasti, kde bude vyžadován, že je tento program efektivní, že má smysl a samozřejmě že má fakulta k dispozici zdroje, které implementaci podpoří a zaštítí.

- **CIO**

Je nezbytné, aby byl na tuto pozici nasazen člověk s potřebnými znalostmi a zkušenostmi, pravděpodobně se bude jednat o zaměstnance z IT oddělení. Ten pak bude spolupracovat s manažerem IT bezpečnosti, aby byl program úplný a správný. Spolu naplánují celkovou strategii SAE programu, jeho implementaci, ujistí se, že vedení fakulty a všem zúčastněným stranám bude vhodně vysvětlen koncept a strategie programu a budou informováni o průběhu implementace. Též se budou muset zpětně ujistit, zda je k dispozici dostatek financí pro spuštění programu.

- **CISO**

Manažerem informační bezpečnosti (CISO) bude jmenován vedoucí IT bezpečnosti na fakultě. Jak je zmíněno výše, bude spolupracovat s CIO a bude dohlížet na včasné a správné zpracování a dodání materiálů pro školení a zvyšování bezpečnostního povědomí ve škole. Bude mít na starosti kontrolu manažerů a bude dohlížet na to, aby měli k dispozici možnost podat adekvátní zpětnou vazbu. Navíc bude v jeho kompetenci dohled nad pravidelnou aktualizací materiálů.

- **Manažeři**

Manažery budou jednotliví vedoucí ústavů (informatiky, financí, managementu a ekonomiky) a jako takoví budou mít na starosti spolupráci s CIO a CISO, budou jim hlásit nedostatky, budou kontrolovat uživatele v rámci svého ústavu, aby byli správně

proškolení a informovaní, aby nedocházelo ke zbytečným chybám z nedostatku pozornosti nebo kvůli nevědomosti.

- **Uživatelé**

V poslední skupině, která je největší, budou všichni zbývající lidé, kterých se bude SAE program týkat. Půjde o studenty, technicko-provozní útvar, návštěvy, hosty, dodavatele a ostatní osoby, které budou potřebovat umožnit přístup do systému školy.

- **Studenti IM se specializací na bezpečnost**

Studenti magisterského programu Informační management jsou speciální skupinou. Od školního roku 2021/2022 se jedná o dvouletou specializaci (po dobu 4 semestrů), jejíž studenti budou mít po splnění určitých podmínek k dispozici certifikát o absolvování kurzu. Znalost studentů této specializace bude odpovídat 3. úrovni SAE programu, kterou je vzdělávání.

3.4.2 Cíle, kterých má být dosaženo

Cíle pro všechny úrovně musí být v souladu s pravidly chování, které by měly být ukotveny v politikách organizace. Tato pravidla by měla platit pro všechny.

Povědomí – V případě povědomí se cílí na velké publikum, které má pasivní roli a je pouze příjemcem informací. Cílem je předat informaci, vytvořit takové materiály, které cílovou skupinu zaujmou, donutí ji jim věnovat pozornost a následně tuto skupinu upozorní na základní informace, které by měli mít, pro zabezpečení svých dat.

Školení – Školení je více formální. Cílem je dosáhnout, aby cílová skupina rozuměla obsahu této úrovně. V rámci školení jsou produkovány informace potřebné pro nabytí potřebných znalostí a dovedností, které skupina potřebuje pro svůj pracovní výkon. Na této úrovni uživatelé získávají praktické znalosti skrze např. lekce, případové studie nebo přímo praxí.

Vzdělávání – Cílem je produkce specialistů a profesionálů na IT bezpečnost, kteří jsou prozíraví a proaktivní a výsledkem by mělo být porozumění problematice IT bezpečnosti. Vzdělávání je dlouhodobý proces.

Profesní rozvoj – Cílem je vyšší odbornost a větší šíře znalostí v oblasti IT bezpečnosti. Většinou se jedná o jednotlivce nebo ne moc početné skupiny. Tato úroveň je potřebná pro osoby, které se IT bezpečnosti věnují profesně.

3.4.3 Frekvence opakování

Jak již bylo zmíněno v teoretické části, SAE program je cyklus vzdělávání a je potřeba jej na základě zpětné vazby, nových průzkumů a novinek v oblasti bezpečnosti aktualizovat.

- Povědomí – Zásady a pravidla pro bezpečí dat (silné heslo, záloha dat aj.) budou stále stejné, tudíž materiály pro zvyšování povědomí nebude potřeba měnit často. Postačující bude jednou za školní rok a to spíše z grafického hlediska, protože jakmile si na tyto materiály návštěvníci, studenti a zaměstnanci fakulty zvyknou, nebudou jim věnovat pozornost. Každopádně bude pro studenty dostupný modul ve školním systému, kde si budou moci procvičit a následně otestovat své znalosti. Tento modul bude aktualizován jednou měsíčně. V rámci semestru bude navíc zavedena jedna odborná přednáška pro každý obor.
- Školení – Každý zaměstnanec bude povinně absolvovat školení jednou za semestr, které povede externí firma. Navíc bude každý měsíc spuštěn test v informačním systému, který bude pro zaměstnance taktéž povinný. Test si budou moci spustit kdykoliv v průběhu týdne. Týden před uplynutím časové lhůty přijde upozorňující email, že test musí složit.
- Vzdělávání – Pro osoby, jichž se bude vzdělávání týkat, platí to samé, co pro školení. Navíc bude pravidelně 1x za semestr společný krátký opakovací kurz, na jehož konci bude prověřovací test. Kurz bude společný pro zaměstnance, kterých se to týká, a pro studenty magisterského oboru Informační management. Těmto studentům budou navíc naplánovány dvě odborné přednášky v průběhu každého semestru mimo klasickou výuku. Přednášky budou vedeny odborníky z praxe.
- Profesní rozvoj – V tomto případě platí stejné podmínky, jako pro vzdělávání (podmínky pro školení + 1x za semestr kurz s prověřovacím testem na konci). Od vzdělávání se bude lišit pouze obsahem informací. V případě, že se bude blížit lhůta platnosti certifikátu, bude potřeba podstoupit podmínky, které povedou k obnově tohoto certifikátu.

V případě povinných přednášek, školení a kurzů bude k dispozici arch, na který se všichni účastníci podepíšou, aby bylo možné sledovat účast.

3.4.4 Návrh struktury SAE

Možností, jak navrhnout, rozvíjet a implementovat SAE program je spousta, ale nejčastěji se užívají tři modely, které byly podrobně popsány v kapitole 1.4.2 Pro Fakultu podnikatelskou bude nejlépe fungovat model, kterým je Částečně decentralizovaný přístup.

Částečně decentralizovaný přístup

Jak již bylo zmíněno v kapitole 1.4.2, model obsahuje centralizovanou politiku a strategie, ale implementace je distribuovaná. Z toho plyne, že implementace neboli realizace modelu je rozdělená na více odpovědných osob, většinou jde o vedoucí jednotlivých úseků. Naopak posuzování potřeb, školení, zvyšování bezpečnostního povědomí a strategie je v režii pověřené osoby. Výhodou tohoto způsobu je komunikace, která mezi vedením organizace a jednotlivými úseky plyne oběma směry.

Obrázek 20: Částečně decentralizovaný přístup
(Zdroj: Vlastní zpracování dle 3, s. 14)

3.5 Rozvoj podpůrných materiálů pro zvyšování povědomí

Jakmile je vytvořený program pro zvyšování bezpečnostního povědomí, mohou se vytvářet podpůrné materiály, které by se měly vytvářet po tom, co se zeptáme na otázku: „Jaké chování chci posílit?“.

Je potřeba materiály sestavit tak, aby byli uživatelé schopni informace z nich získané pak reálně uplatnit, a to jak v práci, tak osobním životě. Program SAE může být efektivní, ovšem je potřeba, aby byly školící materiály zajímavé a aktuální (42, s. 23).

3.5.1 Materiály pro zvyšování povědomí

Je potřeba si nejdříve položit otázku: „Čeho organizace chce, aby si uživatelé byli vědomi ohledně IT bezpečnosti?“. Plán zvyšování povědomí a plán školení by měly obsahovat seznam témat.

Témata pro zvyšování povědomí

Reálně využitá témata pro zvyšování povědomí na Fakultě podnikatelské:

- Tvorba silného hesla, jeho užití a jeho správa
- Ochrana před viry, červy, Trojskými koni
- Jak se zachovat v případě obdržení neznámého emailu s přílohou
- Zálohování dat
- Sociální inženýrství
- Zásady bezpečnosti při cestování
- Pravidelná aktualizace
- Užívání dvou faktorového ověření
- Chování na internetu
- Ochrana účtů na sociálních sítích, zásady zabezpečení

Zdroje pro tvorbu podpůrných materiálů

Existuje spousta různých zdrojů pro tvorbu materiálů, které se využívají pro budování bezpečnostního povědomí. Pro fakultu budou využity tyto:

- Normy, směrnice, právní dokumenty
- Semináře, kurzy
- Emailová upozornění
- Webové stránky pravidelně přidávající informace o IT bezpečnosti
- Audity a interní kontroly

V případě přednášek, kurzů či seminářů, které budou pořádány pro studenty pro zvyšování bezpečnostního povědomí, budou najati externisti. Přednášky budou čistě v jejich režii, to znamená, že i materiály, které na daných přednáškách budou využity, bude mít vybraný externista na starosti.

3.6 Podpůrné materiály pro zvyšování povědomí

Jak již bylo v předchozích kapitolách uvedeno, kromě první úrovně bude vše obstarávat externí firma. To znamená, že materiály pro školení, vzdělávání a profesionální rozvoj bude mít vybraná firma ve své kompetenci, a to včetně obsahu a řízení školení a kurzů. Proto bude obsahem této kapitoly zpracování materiálů pouze pro zvyšování povědomí, které budou ve škole využity (jejich konkrétní příklad bude v přílohách na konci diplomové práce). V rámci kapitoly je řešeno a popsáno několik důležitých témat, která jsou následně obsažena v konkrétních návrzích na konci diplomové práce.

3.6.1 Kybernetická hygiena

Princip je zamýšlen jako analogie k osobní hygieně a jejím cílem je minimalizace kybernetických rizik. Správná kybernetická hygiena může napomoct zvýšení imunity organizace vůči útokům a snížit pravděpodobnost její zranitelnosti (4). Jde o návyky, které by si měl každý člověk vytvořit. Prvním krokem vstříc zabezpečeným datům je prevence.

Bezpečnost mobilních zařízení

Mobily, smartphony a podobná zařízení jsou lákavými cíli, protože nabízí jedinečné možnosti pro hackery, kteří se shání po informacích. Existuje několik různých způsobů, jak vhodně chránit tato zařízení, jako například:

- Užívat pin nebo heslo pro odemčení telefonu a toto heslo pravidelně měnit.
- Ideálně vypnout aplikace, které moc nevyužíváme
- Vyhnout se otevírání souborů, klikání na odkazy nebo volaní na čísla obsažené v nevyžádané zprávě nebo emailu.
- Aktualizovat software, a to jak v případě operačního systému, tak i aplikací.
- Nevyužívat tzv. „Pamatuj si mě“ přihlášení na webových stránkách a mobilních aplikacích – je lepší vždy zadávat přihlašovací údaje.
- Porozumět rizikům, která plynou z užívání těchto zařízení.
- Projít si a pochopit souhlas se zpracováním osobních údajů, co se soukromí a přístupu týče, před nainstalováním aplikací třetích stran.
- Důležité úkony, jako například internetové bankovnictví, provádět pouze ze známého a důvěryhodného prohlížeče (46).

Bezpečnost hesel

Existuje pár zažitých podmínek, které se užívají pro vytváření hesel. Nejčastější podmínkou při vytváření hesla bývá jeho délka. Většinou se lze potkat s podmínkou minimálně 8 znaků. Nejbezpečnější heslo je takové, které se skládá z alespoň 10 znaků, mezi kterými jsou velká a malá písmena, číslice a speciální znaky, jako jsou například dvojtečka, čárka, tečka. Čím lepší bude kombinace, tím odolnější heslo bude.

- Nejlepší je využít zapamatovatelnou frázi a s její pomocí vytvořit silné heslo kombinací různých znaků. Např. „Máme doma dvě kočky, černého Bennyho a bílou Tlapku, kterým je 5 let.“ – z této fráze může vzniknout heslo: „MD2k,čBabT,Kj5L“.
- Při zadávání hesla je potřeba vnímat okolí a vždy si zakrývat klávesnici, na které zadáváme heslo.
- Je potřeba využívat rozdílná hesla pro pracovní a osobní účty.
- Není vhodné zapisovat si hesla do poznámek v mobilu, na lepící papírky k počítači nebo je ukládat přímo v daném zařízení.
- Pokud vznikne jakékoliv podezření, že naše heslo mohlo být odhaleno, je potřeba jednat rychle a změnit si jej.
- Je záhodno měnit si heslo po navrácení z cestování (46).

Email phishing

Phishing je taktika užívaná podvodníky, kteří se snaží získat citlivé údaje (hesla, údaje o platebních kartách, rodná čísla apod.) jednotlivce nebo skupiny na základě toho, kde pracují, co je baví nebo na základě osobních charakteristik. Šíří se podvodnými emaily nebo přesměrováním na falešné webové stránky. Emaily jsou vždy vytvářeny tak, aby cílovou osobu/skupinu zaujaly a aby se zdály, že jsou pro daný cíl nějak zajímavý. Před otevřením přílohy nebo klikání na odkazy, je potřeba, se ujistit, že:

- Odesílatel je důvěryhodný a způsob, jakým je email napsaný, opravdu tomuto odesílateli odpovídá (např. pracovní vedoucí pravděpodobně nebude posílat email s odkazem na video, kde si hrají roztomilá koťátka).
- Obsah je opravdu relevantní k naší práci a není pouze zajímavostí.
- Webová adresa nebo příloha je k obsahu emailu relevantní.
- Osobní emailová adresa odesílatele nebo podezřelá doména jsou správné (46).

Tipy pro používání sociálních médií

- Je vhodné používat rozdílná hesla pro každý účet (na Instagramu, Facebooku, Twitteru, emailu, Snapchatu a podobných médiích).
- Je potřeba se ujistit, že bylo použito všech dostupných možností, jak své účty zabezpečit a ochránit tak své osobní údaje.
- Je potřeba pravidelně kontrolovat zásady zabezpečení a ochrany osobních údajů, jestli nedošlo k nějakým změnám.
- Být obezřetný v případě, že navštěvujeme neznámé webové stránky nebo klikáme na neznámé přílohy.
- Každou podezřelou situaci či incident je potřeba nahlásit IT podpoře.
- Je potřeba se nejdřív pořádně zamyslet, než budeme vkládat osobní informace na sociální média, a to z hlediska jak soukromí, tak i informační bezpečnosti (46).

Cestování s mobilními zařízeními

V případě, že cestujeme kamkoliv mimo naši či pracovní síť je potřeba si uvědomit, že existují jisté kroky, které je potřeba před, během a po cestování podniknout. Tyto kroky vedou ke zvýšení bezpečnosti informací, které máme uložené na mobilních zařízeních (smartphony, notebooky, tablety aj.).

- V některých státech jsou hotelová centra a telefonní sítě monitorovány a pokoje mohou být dokonce prohledávány.
- Vyšší úředníci a ti, kteří pracují s cennými informacemi, jsou náchylnější k zacílení prostřednictvím mobilního zařízení.
- Mobilní zařízení jsou prvním cílem pro zloděje – pokud dojde k jejich krádeži, data, která obsahuje, mohou být zpřístupněna a použita pro škodlivé účely.
- Během cestování je vhodné využít speciální zařízení a ne to, které je využívané pro práci či osobní život.
- Nepoužívat úložná zařízení (např. USB klíče), která jsme dostali nebo zakoupili z neznámých zdrojů.
- Vyhýbat se užívání vlastních USB klíčů na cizích počítačích.
- Používat pouze taková nabíjecí zařízení, která jsme si zakoupili.
- Měnit svá hesla, jakmile se z cesty vrátíme zpátky (46).

Obecné rady pro prevenci

- Pravidelná aktualizace zařízení – mít nainstalovaný nejnovější software, webový prohlížeč a operační systém je nejlepší ochranou proti virům, malwarům a podobným hrozbám. Pokud je to možné, je dobré si zapnout automatické aktualizace.
- Ochrana zařízení připojených k internetu – skvělými způsoby, jak dosáhnout bezpečného zařízení, jsou dvou faktorová autentizace a základní bezpečnostní produkty, jako je antivirus, který chrání zařízení před viry, malwary a neautorizovaným přístupem.
- Wifi sítě – nepoužívat veřejné, neznámé nebo nezabezpečené wifi sítě (46).
- Password manager (správa hesel) – jedná se o aplikaci, která má uložená všechna naše hesla, která si do ní vložíme a která jsou používaná. Do aplikace se lze dostat po zadání hesla (je vhodné mít toto heslo opravdu silné, návod jak jej vytvořit je podkapitole „Bezpečnost hesel“) a splnění určitých podmínek.
- Dvou faktorové ověření – jedná se o kombinaci dvou způsobů, které na sobě nejsou závislé a díky kterým si aplikace ověří identitu uživatele před tím, než mu povolí přístup. Když se uživatel chce například přihlásit do internetového bankovnictví, tak po zadání přihlašovacích údajů mu na telefon přijde potvrzovací SMS s kódem. V dnešní době se používají sofistikovanější způsoby, jako je například biometrické ověření (např. otisk prstu).
- Šifrování – jde o postup, kdy jsou pomocí kryptografie data převedena na data šifrovaná, která lze přečíst pouze pomocí dešifrovacího klíče. V dnešní době jsou již mobilní zařízení s Androidem nebo iOSem v základu šifrována, tudíž se do nich nelze dostat aniž by nebyly odemčeny (nebo je to velice těžké).
- Zálohování – existuje spousta služeb, které se dají bezplatně využít například k zálohování fotek či dokumentů. Též je možné zakoupit externí disk, na který se dané potřebné dokumenty či fotografie pouze z počítače zkopírují. Záloha funguje pouze tehdy, když se dané soubory nachází minimálně na dvou místech najednou. To znamená, že data jsou zálohována tehdy, jestliže jsou přesunuta z počítače na externí disk a na obou zařízeních zůstanou. Pokud jsou data přesunuta a pak z počítače vymazána, tak jsou k dispozici pouze na jednom zařízení, což znamená, že nejsou zálohována.

- Je potřeba být pozorný – jedná se o nejzákladnější pravidlo. Spousta chyb se vyskytne tehdy, kdy je uživatel nepozorný a patřičně se nevěnuje své práci. Je potřeba si všímat, co kde povolujeme, potvrzujeme a na co klikáme. (47)

3.6.2 Pět pravidel pro zaměstnance (a nejen pro ně)

1) Neotvírat přílohy

Je potřeba pravidelně zaměstnancům připomínat, aby neotevírali emaily od odesílatelů, které neznají a které jsou podezřelé. Když už takový email otevřou, za žádnou cenu nesmí klikat na přílohy podezřelého emailu. Většinou jde takový email poznat například podle emailové adresy, případně podle textu v emailu, který většinou obsahuje spoustu chyb. Je potřeba také vědět, že útočníci bývají šikovní a nebezpečný software jsou schopní schovat do souboru, který se jeví jako .pdf nebo .doc.

2) Pravidelně aktualizovat

Firmy vytvářející software nachází jeho chyby a slabiny denně, proto je potřeba aktualizace, ve kterých jsou opraveny tyto chyby a slabiny a díky aktualizacím je daný software bezpečnější.

3) Speciální wifi pro hosty

Je záhodno upozornit zaměstnance, že v případě, že se budou potřebovat připojit k soukromým účtům, tak je vhodné využít wifi pro hosty, protože z počítače, který není připojen k firemní síti, není tak jednoduché se dostat k firemním datům.

4) Vypínat počítač

Pokud by se počítače nechávaly pouze v režimu spánku po tom, co zaměstnanec odejde z práce a již by na něm ten den nikdo pracoval, je stále možné je napadnout. Naopak počítač, který je odpojen od sítě není možné napadnout.

5) Užívat silné heslo

Používání vhodného hesla je snad první věc, kterou by měl člověk znát, pokud má aspoň minimální povědomí o informační bezpečnosti. Většina služeb již má v části registrace podmínku, jak má dané heslo vypadat. Většinou se jedná o minimální počet znaků, pečlivější služby ještě přidávají podmínku kombinace velkých a malých písmen a číslic, ty nejsofistikovanější služby požadují při vytvoření hesla přidat navíc speciální znak. Heslo skládající se z alespoň 8 znaků, přičemž bude heslo obsahovat alespoň jedno velké a malé písmeno, jednu číslici a jeden speciální znak (dvojtečku, čárku, tečku apod.), je považováno za bezpečné heslo.

3.7 Implementace bezpečnostního programu

Implementace může být provedena po stanovení strategie, jakým způsobem se bude program SAE implementovat. Musí být hotová strategie pro vzdělávání a školení a samozřejmě je nutné mít již k dispozici materiály, které budou k implementaci použity.

3.7.1 Komunikace plánu SAE programu

Je nutné začít komunikovat plán SAE programu s osobami, jichž se to dotkne, tedy s uživateli. V tomto případě se tak jedná primárně o zaměstnance a studenty. Program implementace musí být náležitě vysvětlen, což zahrnuje jak očekávané výsledky, které by SAE mělo přinést, včetně přínosů, tak i například objasnění, kdo bude celý proces finančně zajišťovat.

Scénář komunikace podle modelu částečně decentralizovaného přístupu

V tomto případě má zodpovědnost CIO a/nebo manažer programu IT bezpečnosti (CISO). Zodpovídá za rozvoj bezpečnostních politik a také za rozvoj programu SAE. Má na starost posouzení potřeb, od kterého je odvozena strategie. Následně vedoucí jednotlivých úseků obdrží rozpočet pro zvyšování povědomí a školení, vypracují plány programu školení pro vlastní úsek a následně jej implementují. Podle nutnosti pak hlásí aktuální stav CIO a/nebo manažerovi programu IT bezpečnosti.

3.7.2 Metody šíření materiálů pro zvyšování povědomí

Existuje několik způsobů, jakými budou materiály pro zvyšování povědomí šířeny, přičemž fakulta využije některé z nich:

- Plakáty, vizitky, letáky, puzzle, omalovánky – Je potřeba najít vhodné místo, kde se budou tyto materiály nacházet. Místo se musí vybrat s ohledem na pohyb studentů. Strategickými místy pro umístění plakátů jsou nástěnky u obou vchodů fakulty, vstup do knihovny a na stolech u počítačů v knihovně, okolí kantýny a všechny nástěnky v blízkosti stolů s židlemi, které se nachází na chodbách. Na stolech na chodbách, v počítačových učebnách.
- Spořiče obrazovek – Upravené spořiče se budou nacházet na každém počítači, který fakulta má, ať už jde o ty v učebnách nebo v kancelářích zaměstnanců. Spořič se zobrazí ve chvíli, kdy se uživatel ze systému odhlásí.
- Příručka prváka – Do příručky prváka budou vždy přidávány informace ke zvyšování bezpečnostního povědomí, jako například o tom, jak si vytvořit odolné

heslo, že je potřeba pravidelně zálohovat, jak se chovat na internetu a sociálních sítích apod.

- Firemní emaily
- Modul v informačním systému – Bude obsahovat obsáhlejší informace ohledně témat týkajících se bezpečnosti dat, ochrany účtů aj. Pravidelně v něm budou studenti skládat testy.

Podle typu materiálu bude potřeba vytvořit jasná a úderná hesla, v některých případech bude možné prezentovat obsáhlejší zprávu.

3.8 Finanční zhodnocení

Následující kapitola je zaměřena na finanční stránku projektu. Jsou zde finančně zhodnoceny náklady na školení zaměstnanců, na informační kurzy pro studenty, náklady na informační materiály pro zvyšování povědomí. Také bude potřeba vyřešit zavedení bezpečnostního modulu do informačního systému školy, který pro studenty bude obsahovat informace, které patří do základního povědomí o chování na internetu. Pro zaměstnance bude navíc obsahovat základní informace, navíc bude pro každého zaměstnance, který projde školením, každý měsíc dostupný prověřovací test. Tento test bude povinný a zaměstnanec si jej bude moct spustit prakticky kdykoliv v průběhu daného měsíce. Všechny uvedené ceny jsou pouze orientační a nemusí odpovídat realitě, nehledě na to, že se SAE program musí pravidelně aktualizovat a upravovat, tudíž se jedná pouze o počáteční náklady a v tuto chvíli není možné stanovit konečnou částku.

Tabulka 10: Finanční zhodnocení
(Zdroj: Vlastní zpracování)

Název činnosti	Hodinová sazba	Počet hodin	Částka/rok
Analýza současného stavu	600Kč /hod./2 os.	30	18 000,-
Předprojektová fáze	300/hod.	1080	324 000,-
Školení zaměstnanců			340 000,-
Kurzy pro studenty			234 000,-
Podpůrné školící produkty			10 000,-
Vytvoření bezpečnostního modulu	300 Kč/hod/os.	30	45 000,-
Zavedení bezpečnostního modulu	300 Kč/hod/os.	20	30 000,-
Celkem			**1 001 000,-**

Analýza současného stavu – Musí být provedena, protože je nutné vědět, kde jsou chyby a nedostatky a ty pak napravit. Analýza bude provedena oborníky z fakulty, z toho plyne, že není potřeba shánět externí firmu. Tito zaměstnanci budou průzkum provádět v průběhu své klasické pracovní doby. Počítá se s tím, že je to práce nad rámec povinnosti zaměstnanců, tudíž každému zaměstnanci bude připočítána hodina denně, která bude zaplacena 300Kč/hod. za osobu. Předpokládá se, že k analýze budou potřeba dva zaměstnanci.

Předprojektová fáze – Tato fáze je velice obsáhlá. Je do ní zahrnuto stanovení rozsahu změny, rozdělení uživatelů do cílových skupin, stanovení struktury SAE, vytvoření směrnic a politik, vytvoření časového harmonogramu školení, vytvoření doprovodné dokumentace pro uživatele a spousta dalších činností, které je nutné před samotným zaváděním SAE vykonat. Tato část projektu je nejnáročnější, a to jak časově, tak i nákladově. Do této části bude potřeba zahrnout celý Útvar informačních systémů, který na Fakultě podnikatelské spravuje 8 lidí. Jedná se o vedoucího, jeho zástupce, sekretářku, systémového integrátora, dva správce IT, správce serverů a správce sítě. Každý z nich bude ale do projektu přispívat jiným dílem. Po přepočítání hodin navíc pro každého zaměstnance tohoto útvaru vyšlo navýšení denně o 9 hodin pro celý útvar, přičemž nejmenší navýšení dělá 0,5h a největší navýšení je 2h. Hodinové navýšení je přímo úměrné pracovnímu výkonu. Plat se pro každého pracovníka Útvaru informačních systémů trochu liší, nicméně pro jednodušší výpočet je průměrný plat za hodinu stanoven na 300Kč.

Školení zaměstnanců – Pro cílové skupiny budou samozřejmě vedena rozdílná školení. Školení jako takové bude zhruba pro 50 zaměstnanců. Školení bude provádět externí firma, která pak bude moct vydat každému školenému certifikát o absolvování školení. Částka uvedená v tabulce je převzatá z webové stránky firmy, která se specializuje mimo jiné na školení bezpečnosti (51). Je zde uvedená částka 7 800,- Kč za jeden kurz, který by byl vedený online formou a na jehož konci bude závěrečný test. Při zvládnutí testu dostane účastník osvědčení o způsobilosti. Není zde ale informace, pro kolik lidí je možné kurz vytvořit, tudíž předpokládám, že počet lidí, kteří se mohou připojit na online kurz, je neomezený. Kurz je dvoudenní a bude pro zaměstnance povinný, proto bude nakoupeno alespoň 5 kurzů, aby se časově vešli všichni zaměstnanci.

Bude provedeno i odbornější vzdělávání pro vybrané skupiny, které jsou dražší a stojí kolem 20 000,-/os.

Kurzy pro studenty – Každý semestr se pro studenty domluví odborník, který povede jednu obornou přednášku na téma informační bezpečnosti. Studenti oboru IM se specializací na bezpečnost budou mít takových přednášek více. Opět budou přednášky pod vedením externí firmy, proto je v tabulce počítáno se stejnou sazbou, jako v případě školení zaměstnanců. Po propočítání všech oborů, na všech úrovních studia, tím je myšleno bakalářské, magisterské a doktorské, vyšlo celkové číslo zhruba 30 přednášek ročně, a to jak pro prezenční studium, tak i pro kombinované.

Podpůrné školící produkty – Jedná se o nejlevnější položku finančního zhodnocení celé změny. Jde především o letáčky, seznamy se základními body informační bezpečnosti, které by byly dostupné ve formě vizitek, které se vlezou třeba do peněženky nebo obalu od mobilu, takže by byly stále k dispozici. Spadají sem také podpisové archy pro účastníky školení, které by bylo povinné. Navíc by externí firma dodala své školící potřeby, tudíž nebude nutné tolik utrácet za podpůrné předměty. Cena byla odhadnuta na základě zjištění průměrné ceny za letáky, plakáty a vizitky.

Vytvoření bezpečnostního modulu – Na této činnosti bude pracovat 5 lidí z Ústavu informačních systémů, přičemž cena za hodinu je znovu stanovena na 300Kč/hod. Odhad časové doby, než bude modul vytvořen, je 30 hodin, přičemž je zde určitá rezerva.

Zavedení bezpečnostního modulu – V tomto případě se počítá opět s 5 lidmi, jejichž plat za odvedenou práci je stejný, jako byl stanoven dosud. Očekává se, že modul bude zpřístupněný do 20 hodin po jeho vytvoření.

3.9 Post-implementační fáze SAE programu

Jedná se o poslední fázi životního cyklu SAE programu. Pokud se nebude program stále sledovat, vyhodnocovat a aktualizovat, může se rychle stát zastaralým. Proto je potřeba, aby CIO a CISO sledovali aktuální děni v oblasti technologických pokroků, IT infrastruktury a změnám v organizaci. Nejdůležitější částí této fáze je zpětná vazba, díky které jsou pak vedoucí programu schopní jej aktualizovat. Pro hlídání programu a využití zpětné vazby je vhodné vytvořit systém reportů, které budou hlásit závady a mezery

v programu. Bude sestaven plán, jak reporty vyřešit, například úpravou školení či kurzů nebo informováním vedení fakulty, pokud půjde například o administrativní potíže.

3.9.1 Hodnocení programu a zpětná vazba

Jedná se o nejdůležitější část poslední fáze životního cyklu SAE programu a zahrnutí hodnocení a zpětné vazby do programu je přímo kritické. Bez zpětné vazby není možné, aby se program stále vyvíjel a zlepšoval. Způsob zpětné vazby musí být navržen tak, aby splňoval cíle, které byly původně stanovené pro program SAE. Existuje několik způsobů zpětné vazby, pro Fakultu podnikatelskou jsou vhodné:

- Průzkumy, interview
- Nezávislá pozorování
- Hodnotící formuláře a dotazníky
- Benchmarking (stálé porovnávání a měření procesů organizace, které bude provádět CIO a CISO)
- Reportovací systém (hlášení o stavu)

Na konci každé přednášky pro studenty, školení či kurzů pro zaměstnance a vybrané studenty (studenti IM se specializací na bezpečnost) bude každému účastníkovi rozdán krátký dotazník či formulář pro zjištění zpětné vazby. Stejné dotazníky budou k dispozici na strategických místech na fakultě spolu s papírovými schránkami na jejich odevzdání. Dotazníky budou dostupné všem.

3.9.2 Správa změn

Pro správu změn je potřebná nejen zpětná vazba, ale je nezbytné, aby CIO a CISO sledovali vývoj okolí, které program ovlivňuje. Jde o změny v zákonech, vládní nařízení, směny ve směrnicích. To vše má na SAE program vliv a je potřeba jej pak nové situaci přizpůsobit.

3.9.3 Ukazatele úspěšnosti programu

CIO, CISO a další zúčastněné strany, které pomáhají v realizaci programu, by měly být primárními osobami, které budou apelovat za to, aby se SAE program neustále zlepšoval. Důležité je si uvědomit, že ochrana dat a infrastruktury organizace je týmová práce a platí, že bezpečnost je tak silná, jak silný je její nejslabší článek. Pro měření úspěšnosti programu budou využity tyto ukazatele:

- Dostupnost dostatečných finančních zdrojů pro návrh, implementaci a sledování funkčnosti SAE programu.
- Vhodné rozdělení klíčových rolí pro realizaci strategie
- Široká distribuce materiálů (papírové materiály, využití webu, emailu)
- Výše návštěvnosti povinných školících kurzů

Závěr

V úvodu diplomové práce byl stanoven cíl, kterým bylo zpracování práce tak, aby došlo ke zvýšení povědomí o informační a kybernetické bezpečnosti na Fakultě podnikatelské. Tohoto cíle bylo dosaženo. Práce se orientuje na zpracování materiálů a informací převážně pro zvyšování povědomí, které se týká všech zainteresovaných stran. Zpracování materiálů pro školení a vzdělávání a jejich obsah není primární zaměření této práce. Přínosem práce je, mimo jiné, snížení bezpečnostních incidentů, zvýšení konkurenceschopnosti v rámci fakult po celé České republice a zvýšení bezpečnosti dat a informací nejen fakulty, ale i studentů a zaměstnanců.

První oddíl této práce je tvořen teoretickými východisky. Obsahuje vysvětlení základních pojmů, je představeno ISMS, normy a standardy mající vliv na práci. Následuje kapitola o SAE programu a jeho částech. Je zde také zmínka o bezpečnostní politice, Lewinově modelu a analýzách, které jsou podstatné pro stanovení potřebné změny.

Následující oddíl tvoří analytickou část práce. Nejdříve je představena Fakulta podnikatelská a její organizační struktura. Následují samotné analýzy, kterými jsou SLEPTE, PORTE, 7S a SWOT. Poslední kapitolou v tomto oddílu je analýza rizik.

Třetím a posledním oddílem této diplomové práce jsou vlastní návrhy řešení. Nejdříve byl zpracován Lewinův model, díky kterému bylo zjištěno, že je vhodné změnu provést. Následovalo zpracování časové analýzy. V této kapitole je zobrazen graf, díky kterému lze snadno zjistit, jak dlouho bude zhruba projekt budování bezpečnostního povědomí trvat a jaké jsou činnosti, které se nesmí zpozdit, jinak by hrozilo opoždění projektu. Další kapitoly se až do konce oddílu s návrhy řešení věnují samotnému SAE programu. Je zde stanoven cíl programu, strategie, jsou určeny role s konkrétním popisem, kdo je bude zastávat, a jejich odpovědnosti. Byla určena frekvence provádění školení a vzdělávání a aktualizace materiálů pro zvyšování povědomí. V poslední části vlastních návrhů se nachází finanční zhodnocení a post-implementační fáze, která obsahuje informace ke zpětné vazbě.

Seznam použité literatury

1) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.
2) ČSN ISO/IEC 27001, *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*, Praha: Český normalizační institut, 2014.
3) Historie a současnost. *Vysoké učení technické v Brně Fakulta podnikatelská.* [online]. Brno: Vysoké učení technické v Brně, © 2021 [cit. 2021-01-27]. Dostupné z: https://www.fbm.vutbr.cz/cs/o-fakulte/historie-a-soucasnost
4) Review of Cyber Hygiene practices. ENISA, 2016. ISBN 978-92-9205-219-6.
5) Organizační struktura. *Vysoké učení technické v Brně Fakulta podnikatelská.* [online]. Brno: Vysoké učení technické v Brně, © 2021 [cit. 2021-01-27]. Dostupné z: https://www.fbm.vutbr.cz/cs/o-fakulte/organizacni-struktura
6) How the CISO role is evolving. *Csoonline.com* [online]. [cit. 2021-05-14]. Dostupné z: https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html
7) ČSN ISO/IEC 27000. *informační technologie – Bezpečnostní techniky – Systémy řízení informací – Přehled a slovník*. Třetí vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014,
8) Autorizace, oprávnění (Authorization). *Managementmania.cz* [online]. © 2011-2016 [cit. 2021-02-04]. Dostupné z: https://managementmania.com/cs/autorizace
9) Co je GDPR? *Gdpr.cz* [online]. [cit. 2021-02-04]. Dostupné z: https://www.gdpr.cz/gdpr/
10) Osobní údaje. *Gdpr.cz* [online]. [cit. 2021-02-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/osobni-udaje/
11) Vzdělávání. *Czso.cz* [online]. [cit. 2021-04-07]. Dostupné z: https://www.czso.cz/csu/czso/1-vzdelavani
12) Statistiky přijímacího řízení na akademický rok 2020/2021. *Vutbr.cz* [online]. [cit 2021-04-10]. Dostupné z: https://www.vutbr.cz/uredni-deska/statistiky-rizeni?ac=list&rok=2020

13) Statistiky přijímacího řízení na akademický rok 2019/2020. *Vutbr.cz* [online]. [cit 2021-03-29]. Dostupné z: https://www.vutbr.cz/uredni-deska/statistiky-rizeni?ac=list&rok=2019
14) Legislativa a metodické pokyny pro vysoké školy. *Msmt.cz* [online]. [cit. 2021-03-30]. Dostupné z: https://www.msmt.cz/vzdelavani/vysoke-skolstvi/legislativa
15) What's the difference between information security and cyber security? *Itgovernance.eu* [online]. [cit. 2021-03-30] Dostupné z: https://www.itgovernance.eu/blog/en/whats-the-difference-between-information-security-and-cyber-security
16) Vysokoškolský pedagog. Školství, vzdělávání, věda, výzkum. *Platy.cz* [online]. [cit. 2021-03-30]. Dostupné z: https://www.platy.cz/platy/skolstvi-vzdelavani-veda-vyzkum/vysokoskolsky-pedagog
17) Graf EUR / Kč, ČNB, grafy kurzů měn. *Kurzy.cz* [online]. [cit. 2021-03-30]. Dostupné z: https://www.kurzy.cz/kurzy-men/grafy/CZK-EUR/
18) DOSKOČIL, Radek. *Kvantitativní metody: studijní text pro prezenční a kombinovanou formu studia.* Brno: Akademické nakladatelství CERM, 2011. ISBN 978-80-214-4247-4.
19) Česká republika: Politická a ekonomická situace. *Eacea.ec.europa*.eu [online]. [cit. 2021-03-30]. Dostupné z: https://eacea.ec.europa.eu/national-policies/eurydice/content/political-and-economic-situation-21_cs
20) Laboratoře výpočetní techniky. *Vutrb.cz* [online]. [cit. 2021-04-10]. Dostupné z: https://www.fbm.vutbr.cz/cs/pro-studenty/informacni-systemy/laboratore-vypocetni-techniky
21) Odpadové hospodářství. *Mzp.cz* [online]. [cit. 2021-03-30]. Dostupné z: https://www.mzp.cz/cz/odpadove_hospodarstvi
22) Přehled vysokých škol v ČR. *Msmt.cz* [online]. [cit. 2021-03-31] Dostupné z: https://www.msmt.cz/vzdelavani/vysoke-skolstvi/prehled-vysokych-skol-v-cr-3
23) Vysoké školy v Brně. *Brno.cz* [online]. [cit. 2021-03-31]. Dostupné z: https://www.brno.cz/obcan/skolstvi-vzdelavani/vysoke-skoly/
24) Ekonomie a management. *Vysokeskoly.cz* [online]. [cit. 2021-04-10]. Dostupné z: https://www.vysokeskoly.cz/v/ekonomie-a-management/

25) Hodnocení fakulty. *Primat.cz* [online]. [cit. 2021-04-10]. Dostupné z: https://www.primat.cz/fakulta/vysoke-uceni-technicke-v-brne:fakulta-podnikatelska/1673/hodnoceni
26) Ekonomie a management. *Vysokeskoly.cz* [online]. [cit. 2021-03-31]. Dostupné z: https://www.vysokeskoly.cz/v/ekonomie-a-management/region-brno/#results
27) Chceš vyjet nebo se zapojit do zahraniční aktivity na FP? *Vutrb.cz* [online]. [cit. 2021-04-10]. Dostupné z: https://www.fbm.vutbr.cz/cs/zahranicni/studenti
28) Online veletrh pracovních příležitostí iKariéra.cz 2021. *Vutrb.cz* [online]. [cit. 2021-04-10]. Dostupné z: https://www.fbm.vutbr.cz/cs/online-veletrh-pracovnich-prilezitosti-ikariera-cz-2021
29) Státní rozpočet ČR. *Aktualne*.cz [online]. [cit. 2021-04-10]. Dostupné z: https://www.aktualne.cz/wiki/ekonomika/statni-rozpocet-cr/r~i:wiki:3116/
30) Plán realizace strategického záměru. *Vutbr.cz* [online]. [cit. 2021-03-31]. Dostupné z: https://www.vutbr.cz/uredni-deska/strategicke-zamery-fakult/strategicke-zamery-fakult-a-soucasti-f18850/fakulta-podnikatelska-d38254/plan-realizace-strategickeho-zameru-fp-2018-p161470
31) RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-80-214-3510-0.
32) Výroční zpráva o činnosti Vysokého učení technického za rok 2019. *Vutbr.cz* [online] [cit. 2021-04-06]. Dostupné z: https://www.vutbr.cz/uredni-deska/vyrocni-zpravy-vut/vyrocni-zpravy-vut-f18830/vyrocni-zprava-vut-o-cinnosti-za-rok-2019-d200438/vyrocni-zprava-vut-o-cinnosti-za-rok-2019-p192656
33) Kurzy pro zaměstnance. *Lli.vutbr.cz* [online]. [cit. 2021-03-31]. Dostupné z: https://www.lli.vutbr.cz/kurzy-pro-zamestnance
34) Návody. *Vutbr.cz* [online]. [cit. 2021-04-06]. Dostupné z: https://www.vutbr.cz/cvis/navody
35) VUT software. *Vutbr.cz* [online]. [cit. 2021-04-06]. Dostupné z: https://www.vutbr.cz/intra/software
36) Instalace SAP. *Vutbr.sharepoint.com* [online]. [cit. 2021-04-06]. Dostupné z: https://vutbr.sharepoint.com/sites/SAP/SitePages/Instalace-SAP.aspx

37) Cloudové služby. *Vutbr.cz* [online]. [cit. 2021-04-06]. Dostupné z: https://www.vutbr.cz/intra/cloud
38) DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. 2., aktualiz. a dopl. vyd. Praha: Grada, 2012. Expert (Grada). ISBN 978–80–247–4275–5.
39) Analýza vnějšího okolí podniku (SLEPTE). *Altaxo.cz* [online]. [cit. 2021-03-22]. Dostupné z: https://www.altaxo.cz/zacatek-podnikani/zalozeni-spolecnosti/analyza-vnejsiho-okoli-podniku-slepte
40) McKinsey 7S. M*anagementmania.cz* [online]. [cit. 2021-03-24]. Dostupné z: https://managementmania.com/cs/mckinsey-7s
41) SWOT analýza. M*anagementmania.cz* [online]. [cit. 2021-03-29]. Dostupné z: https://managementmania.com/cs/swot-analyza
42) NIST SP 800-50 Building an Information Technology Security Awareness and Training Program. Gaithersburg: National Institute of Standards and Technology, 2003.
43) Cyber security. *Xevos.eu* [online]. [cit. 2021-05-04]. Dostupné z: https://www.xevos.eu/wp-content/uploads/2019/01/produktovy-list-cyber-security.pdf
44) Úvod do kryptografie. *Earchivace.cz* [online]. [cit. 2021-05-05]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/
45) NIST SP 800-16. *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* Gaithersburg: National Institute of Standards and Technology, 2013.
46) Cyber Hygiene. *Cyber.gc.ca* [online]. [cit. 2021-05-05]. Dostupné z: https://cyber.gc.ca/en/guidance/cyber-hygiene
47) Kybernetická hygiena. *Ictblog.cz* [online]. [cit. 2021-05-05]. Dostupné z: https://www.ictblog.cz/kyberneticka-hygiena/
48) Social Engineering. *Imperva.com* [online]. [cit. 2021-05-05]. Dostupné z: https://www.imperva.com/learn/application-security/social-engineering-attack/
49) Bezpečnostní politika. *Managementmania.com* [online]. [cit. 2021-05-05]. Dostupné z: https://managementmania.com/cs/bezpecnostni-politika-security-policy

50) Lewinův třífázový model změn. *Managementmania.com* [online]. [cit. 2021-04-07]. Dostupné z: https://managementmania.com/cs/lewinuv-trifazovy-model-zmen
51) Bezpečnostní povědomí zaměstnance. *Gopas.cz* [online]. [cit. 2021-05-11]. Dostupné z: https://www.gopas.cz/Kurzy/Katalog-kurzu/IT-bezpecnost-a-Hacking/IT-bezpecnost-a-Hacking/Bezpecnostni-povedomi-zamestnance-vstupni-proskoleni-BPZ-A.aspx?subpage=terms
52) Chief Information Officer (CIO). *Investopedia.com* [online]. [cit. 2021-05-14]. Dostupné z: https://www.investopedia.com/terms/c/cio.asp

Seznam obrázků

Seznam tabulek

Přílohy

Návrh plakátu


Jak si vytvořit silné heslo ve třech krocích
1
Vymysli si zapamatovatelnou frázi. Např.: "Máme doma dvě kočky, černého Bennyho a bílou Tlapku, kterým je 5 let."
2
Rozmysli se, jakým způsobem z toho vytvoříš heslo. Třeba první písmena slov, znaky a čísla.
3
Vznikne ti tak heslo: "MD2k,čBabT,Kj5L".

ROZHLÍŽÍŠ SE PŘI PŘECHÁZENÍ ULICE?

PROČ NECHRÁNÍŠ SVÁ DATA STEJNĚ JAKO SEBE?

01

Neprozrazuj nikomu žádné své přihlašovací údaje

02

Vytvoř si pořádné heslo

03

Zálohuj si data

04

Dávej pozor, co se kolem tebe děje

05

Pravidelně aktualizuj svá zařízení

Denně jsou na světě zaznamenány útoky na desítky tisíc účtů

Nebuď jednou z obětí!

01 Používej rozdílné hesla pro každý účet

02 Ujisti se, že jsi pro ochranu svého účtu udělal maximum

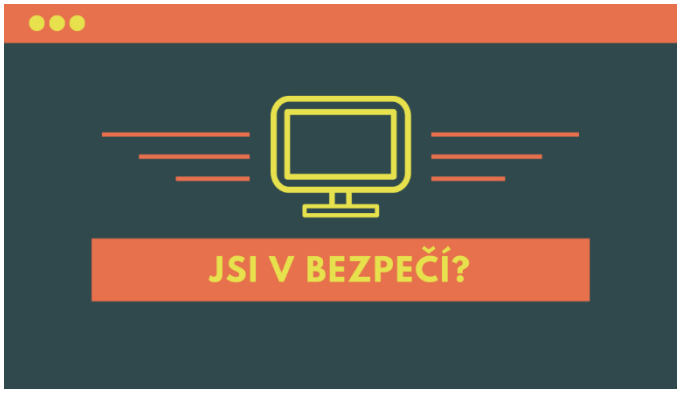
03 Pravidelně kontroluj zásady zabezpečení a ochrany osobních údajů. Nezměnily se?

04 Dávej pozor, když navštěvuješ neznámé stránky nebo klikáš na neznámé přílohy

05 Každou podezřelou situaci nahlaš IT podpoře dané aplikace

06 Pořádně se zamysli, než postneš fotky nebo osobní informace na síť. Nemohl by je někdo využít proti tobě?

Návrhy vizitek



Uvítací obrazovka po odhlášení uživatele/spořič obrazovky